

Law in the Age of Digital Technologies

Edited by Francesca C. Villata,
Mirela Župan, Katarina Trimmings,
Giulia Gabrielli



Milano University Press

Law in the Age of Digital Technologies

Edited by
Francesca C. Villata
Mirela Župan
Katarina Trimmings
Giulia Gabrielli



Milano University Press

Law in the Age of Digital Technologies / Edited by Francesca C. Villata, Mirela Župan, Katarina Trimmings e Giulia Gabrielli. Milano: Milano University Press, 2025

ISBN 979-12-5510-276-2 (PDF)

ISBN 979-12-5510-278-6 (EPUB)

DOI 10.54103/milanoup.215

This volume, and Milano University Press publications in general, unless otherwise specified, are submitted to an external refereeing process under the responsibility of the Milano University Press Editorial Board. The works published are evaluated and approved by the Editorial Board of the publishing house, and must be compliant with the Peer review policy, the Open Access, Copyright and Licensing policy and the Publication Ethics and Complaint policy as reflected in MilanoUP publishing guidelines.

The present work is released under Creative Commons Attribution 4.0 - CC-BY, the full text of which is available at the URL: <https://creativecommons.org/licenses/by/4.0/deed.it>



This and other volumes of Milano University Press are available in open access at: <https://libri.unimi.it/index.php/milanoup>

© The Authors for the text 2025

© Milano University Press for this edition

Published by Milano University Press

Via Festa del Perdono 7 – 20122 Milano

Web Site: <https://milanoup.unimi.it>

e-mail: redazione.milanoup@unimi.it

TABLE OF CONTENTS

Foreword	9

PART 1: THE CONDUCTS OF STATES IN CYBERSPACE: THE INTERNATIONAL LEGAL FRAMEWORK

Navigating Cyberspace: An International Legal Analysis from Regional and Domestic Perspectives	15

Thanapat Chatinakrob

Non-International Armed Conflicts And New Technologies: Reconceptualizing The Intensity Criterion	51

Giulia Baj

Autonomous Navigation and International Law: Does the Principle of Meaningful Human Control Apply at Sea?	79

Daniele Mandrioli

PART 2: THE PRIVATE SPHERE OF DIGITALIZATION

SECTION 1 – CROSS-BORDER BUSINESS TRANSACTIONS

Automated vehicles, tort liability and Private international law	105

Raúl Lafuente Sánchez

Blockchain As a New Vehicle of Electronic Evidence in China	139

Yong Zhang and Qianyi Yan

Smart (Legal) Contracts: New Challenge For North Macedonian Legal System	169

Mirjana Ristovska

Banking and Financial Digital Platforms: Conflict of Laws Issues from a European Perspective	183

Silvia Favalli

A New Form of Working Relationship in The Digital Age: Crowdfunding from a Private International Law Perspective	217

Esra Tekin

The Potential of Digital Markets Act and Digital Services Act to Provide a Meaningful Legal Framework for Collaborative Economy Platforms in the EU	233

Wojciech Lewandowski

Personal Data as Counter-Performance in Exchange for Contents or Services After Amendments to the Italian Consumer Code	255

Sofia Maria Lener

A Lifeguard in Times of Pandemic: Electronic General Meetings in Joint Stock Companies	277

Ufuk Tekin

SECTION 2 – PERSONAL RIGHTS AND FAMILY MATTERS

Circulation of Foreign Public Documents in the Digital Age from a Croatian Legal Perspective	289

Mirela Župan, Paula Poretti and Jura Golub

Facial Recognition Technology in Esports? Youth Protection vs. Human Rights Risks	335

Tsubasa Shinohara

Clinical Risk in Cross-Border eHealth	357

Cristina Campiglio

Legal Challenges for the Regulation of the European Health Data Space	385

Luz M. Martínez Velencoso

Tele-abortion: between privacy and women's reproductive rights	403

Sara Dal Monico

The EU Digital Services Act: An Assessment in Light of the Rights of Persons with Disabilities	427

*Anna Facchinetti **

The Digital Services Act and the Regulation on the Transparency and Targeting of Political Advertising: Initial Reflections	445

Pietro Villaschi

SECTION 3 – CRIMINAL MATTERS

Taking Defence Rights Seriously. The Need for Explainable Artificial Intelligence in Criminal Proceedings – A European Perspective	459

Marcia Michalina

SECTION 4 – THE IMPACT OF DIGITALIZATION ON LEGAL TRAINING

What Every Law Student Should Know About Digitalization. Building a Digital Mindset for Future Lawyers	489

Per Andersen

Foreword

DOI: 10.54103/milanoup.215.c477

This volume is the result of scientific research conducted by a consortium of four partner universities – Aberdeen, Milan, Osijek, and the University of Zagreb Computing Centre – within the framework of the *Time to Become Digital in Law* (DIGinLaw) Project. The Project, fully funded by the European Union under the Erasmus+ programme, was carried out from 1 April 2021 to 30 September 2023.

Taking advantage of the pervasive digital transformations that shape every aspect of our society and lives, the DIGinLaw Project aimed to address the digital demands in higher education and legal research by enhancing the creation and development of digital literacy and competencies that are greatly needed in the legal labour market. The Project aspired to create an open and inclusive society of digital legal knowledge and literacy to benefit lecturers, students, academics, and stakeholders in the legal labour market. To achieve this ambitious goal, the team members participating in the consortium committed themselves to providing high-quality training on digital competencies to students from partner universities and ensuring open access to the results of their joint scientific research on the effects of digitalization on law and legal education.

As part of these efforts, fostered through the continued collaboration and exchange among partners, this volume retraces the scientific research conducted during the Project on the overall theme of the impact of digitalization on law and legal education. It provides opportunities for further discussions on related cross-cutting themes. To do so, it gathers contributions from scholars and researchers from universities worldwide who are experts in various fields within the broader area of legal research.

The pervasiveness and ubiquity of digital technologies and the advent of information society entail multiple transformations and social changes. As digital technologies continue to evolve and permeate countless aspects of social interactions, work relations, political participation, and business and financial transactions, the need to discuss their private, public, cross-border, and international implications becomes urgent. The transformations fostered by digitalization generate new needs, interests, and conflicts that require harmonization and regulation to improve their economic and societal benefits and, most importantly,

limit the risks and negative consequences they might entail for individuals and society at large.

Among the topics addressed in the volume, new legal realities such as collaborative economic platforms, crowdworking, and banking and financial digital platforms raise significant questions about the need for increased transparency, consumer protection, and the protection of human rights. Regarding the new technologies discussed by the featured contributions, Artificial Intelligence (AI)-based systems present some of the most complex legal issues. Facial recognition technologies, automation, eHealth services, and machine-learning each raise specific questions regarding the protection of human rights and fundamental freedoms, especially privacy and personal data, as well as other legal issues such as civil liability and system security. Similarly, transfers in Distributed Ledger Technologies (DLT) are challenging the existing legal framework and introducing new legal phenomena such as smart contracts, prompting wider research and discussions on their regulation, legislation, and the demand for guidance.

The volume acknowledges the need for additional clarity in response to these digital transformations and offers a perspective on a variety of substantive and procedural legal issues. Part 1 focuses on the conduct of states in the so-called cyberspace and touches upon a few selected legal considerations, noting the technical difficulties in applying the existing international legal framework to states' cyber activities, both during peacetime and in times of armed conflict. Part 2 of the volume shifts to the private sphere of digitalization and covers four distinct fields of study. Section 1 addresses cross-border financial transactions, discussing topics such as automation, electronic evidence, and digital platforms from a private international law and European perspective. Section 2 focusses on specific issues arising from digitalization relating to personal rights and family matters, including cross-border eHealth, the circulation of public documents, and the regulation of digital services in light of the protection of human rights and fundamental freedoms. Section 3 explores criminal matters and discusses the integration of AI into criminal proceedings from the perspectives of the right of defense and procedural fairness. Section 4 revisits one of the project's objectives; namely, the impact of digitalization on legal training, and discusses a practical case.

Having outlined the structure of this volume, its rationale, and the objectives of the Project from which the research originated, the editors wish to express their sincere gratitude to the European Commission for the financial support that made the Project possible. Special thanks also go to each team member of the participating universities in the consortium: Josip Juraj Strossmayer University of Osijek (Croatia), University of Milan (Italy), University of Aberdeen (United Kingdom), and the University of Zagreb Computing Centre (Croatia). Lastly, the editors wish to extend their heartfelt gratitude to the

collaborators who worked on the editing process of the volume, particularly Dr. Edoardo Benvenuti, Dr. Sara Bernasconi, Dr. Silvia Favalli, and Dr. Lenka Váľková. Finally, we acknowledge the invaluable contribution of Dr. Giulia Gabrielli for her tireless support in the concept and delivery of this volume.

January 2025

Francesca C. Villata, PhD, Full Professor
Mirela Župan, PhD, Full Professor
Katarina Trimmings, PhD, Professor
Giulia Gabrielli, PhD, Post-Doctoral Fellow

PART 1: THE CONDUCTS OF STATES IN CYBERSPACE:
THE INTERNATIONAL LEGAL FRAMEWORK

Navigating Cyberspace: An International Legal Analysis from Regional and Domestic Perspectives

Thanapat Chatinakrob *

Faculty of Law, Thammasat University, Thailand

ORCID 0000-0003-1680-6247

DOI: 10.54103/milanoup.215.c445

Abstract

Information and communication technologies (ICTs) have become an integral part of modern societies, and their misuse, termed ICT threats, poses an escalating risk to international security and stability. These threats, whether arising from state or non-state actors, can undermine societal progress, economic growth, and human safety. Cyber-attacks targeting critical systems such as energy grids or financial institutions highlight the insufficiencies of current international laws in addressing these challenges. This paper examines legal instruments and policy frameworks that aim to address ICT threats, including those of the European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and the Association of Southeast Asian Nations (ASEAN). However, the enforcement of such regional regulations, policies, and recommendations is yet to be adequately enforced. From a domestic perspective, this paper has explored examples of legal instruments and policy frameworks from various countries, such as the UK, Germany, France, Finland, and Singapore. These examples demonstrate how different countries address ICT threats in their way and how they regulate cyber activities to ensure the security and stability of their respective digital domains. This paper underscores the pressing need for robust legal instruments and policy frameworks that can effectively address ICT threats and

* This is an excerpt from the full research report titled 'the application of international law to cyberspace: the dilemma of state sovereignty violation, extraterritorial effects and cyberspace sovereignty', which is funded by the Research Promotion Committee of the Faculty of Law, Thammasat University. Another part of this full research, different from the current part, was published in Chinese Journal of International Law, Volume 23, Issue 1, March 2024, Pages 25-72. Any errors are the author's own.

safeguard state sovereignty in cyberspace. The review of regional and domestic legal instruments and policy frameworks provides a starting point for identifying the most effective strategies to counteract ICT threats and ensure digital security and stability for all.

Keywords

Cyberspace; International Law; Regional and Domestic Laws and Policy Framework; State Sovereignty Violation; Extraterritorial Effects; Cyberspace Sovereignty.

1. Introduction

The rapid evolution of information and communication technologies (ICT) has been significantly altered global interactions, presenting unparalleled opportunities and pressing challenges. In recent years, ICTs have become indispensable tools for daily operations across industries and societies. Events like the COVID-19 pandemic and ongoing geopolitical conflicts, including the Russia-Ukraine war, have emphasised their critical role. However, these developments also reveal vulnerabilities, as ICT threats have emerged as significant issues for global security.

ICT threats involve malicious actions by State and non-State actors, posing serious risks across various sectors.¹ These threats can be categorised into three primary groups. The first consists of cybercrimes targeting critical infrastructure,² disrupting public services³ and undermining economic stability.⁴ The second includes covert state-sponsored campaigns designed to destabilise systems, jeopardising international peace and causing harm to individuals.⁵ Lastly, the third group involves terrorist activities that exploit ICTs to conduct attacks, recruit members, and incite violence, thereby threatening global peace and stability.⁶

Currently, there is no comprehensive international legislation specifically designed to address ICT-related risks, particularly those associated with state-sponsored cyber threats. Instead, existing international legal frameworks, such as Article 2(4) of the UN Charter, principles of sovereignty and non-intervention, and international human rights law, are applied to regulate cyber

1 UN General Assembly, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135, paras 6–14 [hereinafter GGE 2021 Report].

2 *ibid* para 8.

3 *ibid* para 10.

4 *ibid*.

5 *ibid* para 9.

6 *ibid* para 13–14.

activities. However, these frameworks are not specifically tailored to address the complexities of cyberspace. For instance, the Group of Governmental Experts (GGEs) has made notable contributions in recommending voluntary norms for responsible state behaviour in cyberspace, yet these recommendations remain non-binding and lack enforceability.⁷

Regional efforts have provided some legal instruments to address cyber-related issues. The Budapest Convention on Cybercrime, for instance, facilitates collaboration among signatory states to combat cybercrime by harmonising domestic laws and improving investigative measures.⁸ In contrast, the African Union Convention on Cyber Security and Personal Data Protection has yet to come into force, though its aim is to establish a robust cybersecurity framework for Africa by regulating electronic transactions and protecting personal data.⁹

On a broader scale, international organisations have recognised the pressing need for governance in cyberspace. The United Nations Resolution 73/266 advocates for peaceful ICT use, conflict prevention arising from ICT misuse, and education about technological advancements.¹⁰ Similarly, the European Union (EU) has developed a Cybersecurity Strategy to enhance cooperation among Member States,¹¹ while the ASEAN Cybersecurity Cooperation Strategy aims to bolster regional collaboration.¹² However, such initiatives often lack legal enforceability, limiting their effectiveness.

Despite these efforts, ICT threats remain pervasive, exposing gaps in international legal frameworks and state-level responses. These challenges highlight the need to reexamine foundational principles of international law, particularly

7 *ibid* paras 1–98.

8 Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS 185 [hereinafter Budapest Convention].

9 African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) [hereinafter Malabo Convention].

10 UN General Assembly, ‘Resolution adopted by the General Assembly on 22 December 2018: Advancing responsible State behaviour in cyberspace in the context of international security’ (2 January 2019) UN Doc A/RES/73/266 [hereinafter GGE 2019 Report].

11 European Union, ‘Cyberspace: Strengthening cooperation in promoting security and stability’ (European Union External Action, 17 May 2021) <https://www.eeas.europa.eu/eeas/cyberspace-strengthening-cooperation-promoting-security-and-stability_en> accessed 2 March 2023; European Commission, ‘New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient’ (European Union Press Release, 16 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391> accessed 2 March 2023.

12 ASEAN Secretariat, ‘Joint Media Statement’ (ASEAN, 28 January 2021) ‘The 2nd ASEAN Digital Ministers’ Meeting and Related Meetings’ <<https://asean.org/wp-content/uploads/2022/01/2nd-ADGMIN-Joint-Media-Statement.pdf>> accessed 2 March 2023; ASEAN Secretariat, ‘ASEAN Cybersecurity Cooperation Strategy (2021–2025)’ (ASEAN) <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf> accessed 2 March 2023.

state sovereignty. The issues arising from ICT threats can be categorised into three main areas.

First, ICT threats pose direct challenges to state sovereignty by targeting critical infrastructure. Even when such threats originate outside a state's territory, states may be held accountable for failing to mitigate or counteract them.¹³ The GGEs report emphasises the need for states to prevent the misuse of their territories for illicit ICT activities¹⁴ and to assist other states in responding to cyber incidents.¹⁵

Second, the enforcement of cyberspace regulations often encounters jurisdictional complexities. The transnational nature of ICT activities necessitates the development of harmonised rules that are enforceable across borders. However, such regulations may inadvertently infringe upon the sovereignty of other states, underscoring the need for carefully crafted legal instruments that respect international norms. Third, the concept of cyberspace sovereignty has gained prominence as states assert control over their digital domains.¹⁶ While traditional notions of sovereignty pertain to territorial and governmental authority, cyberspace sovereignty extends these principles to the digital realm. This evolving concept warrants further exploration, especially given the increasing frequency of cyber incidents, such as the 2007 Estonia cyberattack¹⁷ and the cyber dimensions of the 2022 Russia-Ukraine conflict.¹⁸

2. Legal considerations in cyberspace

In recent years, the growing use and reliance on cyberspace have raised several legal issues under international law. The infringement of State sovereignty, extraterritorial impacts, and cyberspace sovereignty are among the major concerns. These challenges have led to questions about the application of conventional international law principles to cyberspace, as well as the need for novel legal frameworks to regulate cyberspace activities.

The infringement of State sovereignty in cyberspace poses a significant threat to fundamental international law principles. Since time immemorial, States have enjoyed exclusive control over their territories and actions. However, cyberspace

13 GGE 2021 Report (n 1).

14 *ibid*, norm 13 (c).

15 *ibid*, norm 13 (h).

16 Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) (1945) 1 UNTS XVI, art 2(1) [hereinafter UN Charter].

17 Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia' (*The New York Times*, 29 May 2007) <<https://www.nytimes.com/2007/05/29/technology/29estonia.html>> accessed 4 March 2023.

18 Center for Preventive Action, 'Conflict in Ukraine' (*Global Conflict Tracker*, updated 12 May 2022) <<https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine>> accessed 4 March 2023.

presents a novel challenge to this notion. As cyberspace activities often transcend national boundaries, it becomes difficult to establish jurisdiction and applicable laws. This increases the likelihood of State sovereignty violations where the actions of one state may encroach on the sovereignty of another.

The impact of activities outside a state's territory is a legal issue in cyberspace. The notion of territorial sovereignty limits State authority to actions that take place within its borders. In contrast, cyberspace activities outside of a State's borders can have significant consequences inside the State. An instance is the destruction of critical infrastructure by a cyberattack from another State, leading to a violation of the targeted State's sovereignty. The extraterritorial effect of online operations has raised concerns regarding the application of established international law principles in cyberspace.

As ICT threats proliferate, they bring to the fore significant legal challenges under international law. The transboundary nature of cyberspace activities necessitates innovative approaches to address state sovereignty infringements, extraterritorial impacts, and the emerging concept of cyberspace sovereignty. The following sections analyse these critical issues in detail.

2.1 State sovereignty violation

Under international law, the principle of State sovereignty mandates that states exercise control within their territories without external interference.¹⁹ Although 'territory' refers to both legal and political notions as well as physical or geographic areas,²⁰ the term can be extended to include regions that lack physical or geographical boundaries but possess legal components such as application, prescription, enforcement, and adjudication that may impact a State's sovereignty.²¹ However, cyberspace presents unique challenges to this principle.

19 Jens Bartelson, *A Genealogy of Sovereignty* (CUP 1993) 26; Montevideo Convention on the Rights and Duties of States (concluded 26 December 1933, entered into force 26 December 1934) 165 LNTS 19; Daniel Bethlehem, 'The end of geography: the changing nature of the international system and the challenge to international law' (2014) 25 *European Journal of International Law* 9, 13; Nicolas G Onuf, 'Sovereignty: Outline of a conceptual history' (1991) 16 *Alternatives: Global, Local, Political* 425, 437.

20 Nicholas Tsagourias, 'The Legal Status of Cyberspace: Sovereignty Redux?' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 13; Thomas Forsberg, 'Beyond sovereignty, within territoriality: Mapping the space of late-modern (geo) politics' (1996) 31 *Cooperation and Conflict* 355, 355; *Island of Palmas (United States of America v Netherlands)* [1928] RIAA 839; Richard T Ford, 'A history of jurisdiction' (1999) 97 *Michigan Law Review* 843, 853–854; John G Ruggie, 'Territoriality and beyond: Problematising modernity in international relations' (1993) 47 *International Organisation* 139.

21 Tsagourias, *ibid*; Frederick A Mann, 'The doctrine of international jurisdiction revisited after twenty years' in *Recueil Des Cours* (Martinus Nijhoff 1984); Peter J Taylor, 'The state as container: Territoriality in the modern world-system' (1994) 18 *Progress in Human Geography* 151, 151.

Cyber-attacks and ICT enabled activities often transcend physical borders, resulting in violations of sovereignty through acts such as data breaches, critical infrastructure sabotage, or disinformation campaigns. Addressing these violations requires clarifying the scope of sovereignty in the digital realm and establishing norms for state behavior in cyberspace.

With the current international regulations concerning cyberspace, particularly the illegitimate usage of ICT, it is observed that such actions may infringe upon other States' sovereignty. A crucial challenge in applying international law to cyberspace is determining whether it can be enforced within a State's territory.

The study conducted by GGE acknowledged the relevance of international law, specifically the UN Charter, in regulating State sovereignty principles in cyberspace. The Group emphasised that the conduct of ICT-related activities by States and their jurisdiction over ICT infrastructure within their territory should be subject to State sovereignty and related international norms and principles. The current obligations under international law are also applicable to States' ICT-related activities.²²

This illustrates that ICT-related activities, despite not being carried out on the territory of another State, can violate the sovereignty of another State. States can exercise their sovereignty by exerting authority over individuals in their territory and over cyber infrastructure located in their territory, including their citizens residing within their sovereign area.²³ This can lead to passive nationality jurisdiction, which may result in activities that infringe on the sovereignty of other States.

The use of sovereignty in cyberspace should have limited legal implications and scope.²⁴ States have sovereignty over their information and communications technology infrastructure within their territory, but this use of sovereignty must not infringe on the sovereignty of another State. The use of ICT must not jeopardise other States' cyber infrastructure, especially cyberattacks on critical infrastructure that threatens the sovereignty of other States.²⁵ Such actions may

22 GGE 2021 Report (n 1) para 71 (b).

23 C-131/12, *Google Spain SL v Agencia Española de Protección de Datos* [2014] ECLI:EU:C:2014:317, paras 32–41; *Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v Belgium)* (Joint Separate Opinion of Judges Higgins, Kooijmans and Buergerthal) [2002] ICJ Rep 3, para 47.

24 US Department of Defense, 'DOD General Counsel Remarks at US Cyber Command Legal Conference' (Speech, 2 March 2020) <<https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>> accessed 8 March 2023; Brian Egan, 'International law and stability in cyberspace' (2017) 35 *Berkeley Journal of International Law* 169, 169.

25 Nicholas Tsagourias (n 20) 22; Finland, 'Finland's national positions: international law and cyberspace' <<https://um.fi/documents/35732/0/cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859>> accessed 10 March 2023, 2–3; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion)

support another State's sovereignty over its territory. Thus, any unauthorised or unjustified operation that interferes with a State's sovereign rights violates the principle of sovereignty, regardless of the degree of interference or damage, physical or non-physical effects, or whether the operation targets governmental services and infrastructure.²⁶

2.2 Extraterritorial effects

The extraterritorial impact of cyber activities is another pressing concern. Actions originating in one State can cause significant harm in another, raising questions about jurisdiction and accountability.²⁷ Existing international legal frameworks often struggle to accommodate the dynamic and borderless nature of cyberspace. This section explores how extraterritoriality can be addressed through enhanced international cooperation, harmonised legal standards, and mechanisms for cross-border enforcement.

The issue of jurisdiction is crucial in cyberspace. The territorial boundaries of a State usually establish its jurisdiction in the physical world. However, with data and communications traversing multiple countries, determining the location of a particular action or participant in cyberspace can be challenging. Consequently, some argue that traditional jurisdictional concepts are inadequate in the digital environment and new approaches are necessary to ensure the effectiveness of international law in governing cyberspace.²⁸ The advancement of technology in various types of cyber activity, such as internet-based defamation, is one of the main reasons for the spread of significant extraterritoriality.²⁹ Many cyber acts are difficult to geographically pinpoint, which means that States may enact internally applicable laws only after considering other factors. These factors may include the effect on persons of their nationality, which may lead to the unlimited right of jurisdiction,³⁰ and the consequences in the

[1996] ICJ Rep 226, 393–394 (Dissenting Opinion of Judge Shahabuddeen); NCSC, 'UK and allies expose Russian attacks on coronavirus vaccine development' (NCSC, 16 July 2020) <<https://www.ncsc.gov.uk>> accessed 10 March 2023; Russell Buchan, *Cyber Espionage and International Law* (Hart 2018) 48–69.

26 Finland, *ibid* 2; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1986] ICJ Rep 14, paras 205 and 247.

27 Hannah L Buxbaum, 'The Practice(s) of Extraterritoriality' in Hannah L Buxbaum and Thibaut Fleury Graff (eds), *Extraterritoriality* (Hague Academy of International Law, Brill 2022) 3.

28 Michael N Schmitt, 'International Law in Cyberspace' (2013) 7 (1) *Journal of National Security Law & Policy* 1, 1–51.

29 Victor Stoica, 'Testing the Continued Viability of Traditional Jurisdictional Norms: The Challenges of Cybersecurity' in Hannah L Buxbaum and Thibaut Fleury Graff (eds), *Extraterritoriality* (Hague Academy of International Law, Brill 2022) 525–570.

30 Vaughan Lowe, *International Law* (OUP 2007) 174; Bruno Simma and Andreas Th Müller, 'Exercise and Limits of Jurisdiction' in James Crawford and Martti Koskenniemi (eds),

form of serious crimes under international law under universal jurisdiction.³¹ Additionally, the impact may be prioritised, and domestic legislation within the country may have cross-border effects.

Another aspect of the extraterritorial effects of international law in cyberspace relates to State responsibility. States are obligated under international law to avoid infringing on the rights of other States and to compensate victims for their actions. Nonetheless, in the cyberspace context, identifying particular actions carried out by a single State can be difficult because they may be performed by non-State actors, necessitate the use of intermediaries, or entail routing through various States. Thus, alternative methods of establishing state responsibility in cyberspace, such as the notion of state responsibility for cyber operations, have been suggested.

Furthermore, there are worries about the application of domestic laws outside a state's territory in cyberspace. Usually, domestic laws are limited to the jurisdiction of a single State, but with data and communications traversing multiple countries in cyberspace, it can be challenging to determine which laws should govern specific conduct. As a result, there have been calls for increased international cooperation to ensure that the extraterritorial application of domestic laws does not result in conflicts or breaches of international law.³²

The issue of extraterritoriality of international law in cyberspace is closely related to the topic of human rights in the digital realm. While the internet and other digital technologies have increased people's ability to communicate and access information, they have also raised concerns about privacy, freedom of expression, and other basic rights. To protect individuals from rights violations in this digital world, it has been suggested that international human rights laws should be extended to cyberspace.

The GGE report fails to address the issue of extraterritoriality, which can have severe consequences in the context of ICT-related activities. For instance, actively hacking a computer system located on a server beyond a State's territorial limits could harm a computer system in another country.³³ Furthermore, States may create domestic legislation to address cyber concerns within their borders, imposing obligations on other States. This may have an effect even if authorities stationed in other States do not access the territory of such enforcing

Cambridge Companion to International Law (CUP 2012) 134, 141–142; Michael Akehurst, 'Jurisdiction in International Law' (1973) 46 *British Yearbook of International Law* 145, 156.

31 Stephen Macedo et al, *Princeton Principles on Universal Jurisdiction* (Program in Law and Public Affairs 2001) 24; *Arrest Warrant* (n 23), 10–11.

32 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006) 154–158 and 165–167.

33 Mireille Hildebrandt, 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace' (2013) 63 (2) *The University of Toronto Law Journal* 196, 197.

States. Consequently, the State may be subject to domestic law restrictions applicable in the territory of other States.

In summary, the extraterritorial effects of international law in cyberspace are complex and expanding, encompassing significant challenges related to jurisdiction, state responsibility, extraterritorial application, and human rights. Although scholars and experts are debating the best approach to address these issues, it is clear that novel methods are necessary to effectively regulate cyberspace under international law. Many international or regional laws, policies, or suggestions still require full implementation.

2.3 Cyberspace sovereignty

The discovery that cyberspace activities can affect both sovereignty and extraterritoriality across borders has led to suggestions for separating cyberspace from domestic law. Chinese President Xi Jinping has promoted the concept of cyber sovereignty, which defines a State's territory as the area in which it can exercise sovereignty.³⁴ A State's network refers to the ICT infrastructure composed of ICT systems built within its territory. This raises the issue of the extent to which States should be allowed to exert sovereignty over their ICT infrastructure.³⁵

The concept of cyberspace sovereignty has gained traction as States seek to assert control over digital activities within their territories. This encompasses regulating data flows, securing critical infrastructure, and protecting citizens' digital rights. However, achieving a balance between State control and the inherently global nature of cyberspace remains a challenge.³⁶

Defining cyberspace as a territory brings about cyberspace rights and duties. It grants cyberspace sovereignty, which entails basic rights to the territory. These rights comprise cyberspace independence, cyberspace equality, cyberspace self-defence, and cyberspace jurisdiction.³⁷

The distinct nature of cyberspace poses a significant challenge in determining the issue of cyberspace sovereignty. Being a virtual realm with no tangible borders and constantly evolving, it's hard to define or set limits to it, making it

34 Ministry of Foreign Affairs of the People's Republic of China, 'Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference' (Wuzhen, 16 December 2015) <<https://www.fmprc.gov.cn>> accessed 14 March 2023; Michael Kolton, 'Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence' (2017) 2 (1) *The Cyber Defense Review* 119, 119; Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realization' in Dennis Broeders and Bibi van den Berg, *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020) 107–142; Binxing Fang, *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace* (Springer 2018).

35 Binxing Fang, *ibid* 83.

36 *ibid*.

37 *ibid* 84.

challenging for authorities to regulate the internet within their territories. Also, as the Internet is a global network accessed by individuals and entities worldwide, no single state can claim complete authority over the entire network.

The absence of established international legal rules and principles that apply to cyberspace presents a further challenge to resolving issues of cyberspace sovereignty. Although several international agreements and conventions exist on internet-related issues, such as the World Summit on the Information Society (WSIS)³⁸ and the GGE 2021 report,³⁹ there is no consensus on how these agreements should be implemented in cyberspace.

It can be argued that ICT threats can have effects that span from State sovereignty to cyberspace sovereignty. The idea of sovereignty in international law, particularly concerning State sovereignty, is important as it deals with the concept of sovereignty in terms of possessing territories, populations, and regimes within one's borders.

3. Existence of regional and domestic legal instruments and policy framework in cyberspace

The rapid emergence and ever-evolving nature of cyberspace have resulted in significant legal and policy challenges, given the increasing reliance of states and societies on digital technology. To address the complexities and dynamism of this environment, various international, regional, and domestic legal instruments and policy frameworks have been established. This article examines the presence of different tools and frameworks that can be categorised as either regional or domestic.

A number of regional organisations have established cyberspace-related legal and policy instruments. The European Union,⁴⁰ for example, has produced a number of directives and rules aimed at preserving individuals' privacy and security in the EU, including the General Data Protection Regulation (GDPR)⁴¹ and the Network and Information Systems Directive (NIS2 Directive).⁴² The

38 International Telecommunication Union (ITU), *WSIS+10 Statement on Implementation of WSIS Outcomes and the WSIS+10 Vision for WSIS Beyond 2015* (ITU 2014) 9–48.

39 GGE 2021 Report (n 1).

40 European Union (n 11).

41 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing Directive 95/46/EC [hereinafter GDPR].

42 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333.

Association of Southeast Asian States (ASEAN)⁴³ has also produced the ASEAN Regional Forum (ARF) Work Plan on Security of and in the Use of Information and Communication Technologies,⁴⁴ with the goal of promoting conversation and cooperation on cyberspace-related problems.

At the domestic level, States have developed a range of legal and policy frameworks to address the challenges posed by cyberspace. These frameworks often cover a range of issues, including the protection of critical infrastructure, the prevention and investigation of cybercrime, and the regulation of the use of digital technologies by individuals and organisations. For example, the UK⁴⁵ has enacted a number of laws and regulations, including the Computer Misuse Act,⁴⁶ which criminalises unauthorised access to computer systems, and the Data Protection Act,⁴⁷ which regulates the processing of personal data. The UK has also established a National Cyber Security Centre,⁴⁸ which serves as the primary authority for cybersecurity issues in the country. The centre is responsible for providing guidance to organisations and individuals on how to protect their networks, and for coordinating the response to cyber incidents.

3.1 Regional laws and policy frameworks in cyberspace

In response to the growing importance of cyberspace in everyday life, regional legal and policy frameworks have arisen. These frameworks seek to improve cyberspace security, stability, and collaboration by addressing the specific issues that the digital realm presents. In this environment, some regional organisations have developed legal tools and policy frameworks to govern cyberspace activity in their particular territories. The European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and the Association of Southeast Asian Nations (ASEAN) have all built regional legal and policy frameworks.

43 ASEAN Secretariat (n 12); ASEAN Secretariat, 'ASEAN Leaders' Statement on Cybersecurity Cooperation' (ASEAN, 27 April 2018) The 32nd ASEAN Summit <<https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/>> accessed 14 March 2023.

44 ASEAN Secretariat, 'ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)' (ASEAN, 7 May 2015) <<https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf>> accessed 14 March 2023.

45 Foreign, Commonwealth & Development Office, 'Application of international law to states' conduct in cyberspace: UK statement' (Policy Paper, 3 June 2021) <<https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement>> accessed 15 March 2023.

46 Computer Misuse Act 1990, UK Public General Act 1990, c.18.

47 Data Protection Act 2018, UK Public General Act 2018, c.12.

48 National Cyber Security Centre, 'The National Cyber Security Centre' (NCSC) <www.ncsc.gov.uk/> accessed 16 March 2023.

The European Union has led regional attempts to control cyberspace activities. The EU has established a number of legal instruments, including the General Data Protection Regulation (GDPR),⁴⁹ the Network and Information Security Directive (NIS2 Directive),⁵⁰ and the Cybersecurity Act,⁵¹ which establish a comprehensive legal framework for cybersecurity and data protection in the region. The GDPR, for example, establishes a uniform set of standards for the handling of personal data, whilst the NIS Directive strives to improve the cybersecurity of network and information systems throughout the EU. In contrast, the Cybersecurity Act establishes a European cybersecurity certification system to encourage a consistent level of cybersecurity throughout the EU.

Similarly, the OAS has created legal mechanisms to govern cyberspace activities in its Member States. In 2007, the OAS held a meeting of a group of governmental experts on cybercrime to strengthen and consolidate cooperation in the prevention and fight against cybercrime, leading to several workshops on cybercrime and the Inter-American Cooperation Portal on Cyber-Crime.⁵² The OAS provided the Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas (REMJA) to conclude existing cyber-crime legislation of the OAS Member States.⁵³ The OAS has also implemented the principles from the Council of Europe's Convention on Cyber-Crime.⁵⁴ Member States are required by the convention to criminalise specific cyber acts, such as illegal access to computer systems, electronic communication interception, and computer-related fraud.⁵⁵ Furthermore, the OAS has established the Inter-American Committee against Terrorism (CICTE) Cybersecurity Program,⁵⁶ which offers Member States technical help and capacity-building on cybersecurity-related issues.

The OSCE has also developed a framework for collaboration among its Member States in order to improve cyber security and stability. In 2012, the OSCE endorsed confidence-building measures (CBMs) in cyberspace, which outline voluntary actions to improve transparency and minimise the danger of

49 GDPR (n 41).

50 NIS 2 Directive (n 42).

51 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151.

52 OAS, 'The Inter-American Cooperation Portal on Cyber-Crime' (Cybercrimedata AS) <www.cybercrimelaw.net/OAS.html> accessed 16 March 2023.

53 Department of Legal Cooperation, OAS, 'OAS Member State Legislation' (OAS) <http://www.oas.org/juridico/english/cyber_legis.htm> accessed 16 March 2023.

54 Budapest Convention (n 8).

55 Department of Legal Cooperation, OAS (n 53).

56 US Department of State, 'Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)' (US Department of State) <<https://2001-2009.state.gov/s/ct/intl/io/cicte/index.htm>> accessed 24 March 2023.

conflict in cyberspace.⁵⁷ The OSCE later adopted new OSCE CBMs in 2016.⁵⁸ The CBMs contain procedures for information exchange, cyber incident notification, and confidence-building measures such as the establishment of hotlines and collaborative cybersecurity exercises among Member States.

Finally, ASEAN has recognised the importance of regional collaboration in cyberspace. In 2018, ASEAN ratified the ASEAN Framework on Digital Data Governance,⁵⁹ which establishes a set of regional data governance standards. The agreement includes measures for personal data protection, cross-border data flows, and Member-State cybersecurity cooperation. Moreover, ASEAN has created the ASEAN Ministerial Conference on Cybersecurity,⁶⁰ which serves as a forum for Member States to debate cybersecurity challenges and foster cooperation in this field.

3.1.1 European Union (EU)

The EU has put in place a number of policies and legislative frameworks aimed at boosting cybersecurity, protecting individuals' rights and liberties, and stimulating economic development and innovation in cyberspace.

The EU's Cybersecurity Strategy, which was released in 2013,⁶¹ outlines a comprehensive strategy for addressing cybersecurity concerns. The strategy's

57 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection' (CCDCOE) <<https://ccdcOE.org/incyber-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/>> accessed 24 March 2023; OSCE Permanent Council, 'Decision No. 1039 Development of Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (26 April 2012) PC.DEC/1039.

58 OSCE Permanent Council, 'Decision No. 1202 OSCE Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202.

59 ASEAN Secretariat, 'Framework on Digital Data Governance' (ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), 6 December 2018) <https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf> accessed 25 March 2023.

60 Government of Singapore, 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2020' (CSR Singapore, 7 October 2020) <<https://www.csa.gov.sg>> accessed 25 March 2023; Nur Azha Putra, 'Is ASEAN Doing Enough to Address Cybersecurity Risks?' (*The Diplomat*, 6 March 2018) <<https://thediplomat.com/2018/03/is-asean-doing-enough-to-address-cybersecurity-risks/>> accessed 25 March 2023.

61 Jorinda Vela, 'The Development of the EU Cyber Security Strategy and its Importance' (FINABEL European Army Interoperability Centre, 2 August 2021) <<https://finabel.org/info-flash-the-development-of-the-eu-cyber-security-strategy-and-its-importance/>> accessed 26 March 2023; Commission, High Representative of the Union, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee

major goal is to keep the EU's digital single market open, safe, and secure.⁶² It identifies five strategic priorities: creating cyber resilience, promoting cybersecurity standards and certification, establishing a cybercrime and incident response network, expanding cyber defence capabilities, and boosting international collaboration.

The EU has also proposed numerous legal measures to achieve the cybersecurity plan, notably the Network and Information Security Directive (NIS2 Directive),⁶³ which went into force in 2018. The NIS2 Directive intends to provide a high degree of cybersecurity throughout the EU's vital infrastructure and important services, such as energy, transportation, banking, and health.⁶⁴ The NIS2 Directive requires member states to identify critical infrastructure operators and develop a national cybersecurity framework.⁶⁵ In addition, the Directive requires these operators to apply suitable security measures, disclose security events, and collaborate with relevant authorities.⁶⁶

The EU also implemented the GDPR,⁶⁷ which came into force in 2018, to safeguard individuals' basic rights and freedoms in the handling of personal data. The GDPR provides standards for personal data collection, use, storage, and transfer, as well as imposing duties on enterprises that process such data. Individuals can also use the regulation to exercise their rights to access, modify, and delete their personal data.

Furthermore, the EU has established the European Union Agency for Cybersecurity (ENISA), which acts as the Union's cybersecurity competence centre. The primary duties of ENISA are to provide guidance and advice to Member States and EU institutions, to support the formulation and implementation of the EU's cybersecurity strategy, and to promote cooperation and information sharing among Member States.⁶⁸

In summary, the EU has put in place a comprehensive legal and regulatory framework to address cybersecurity concerns, safeguard individuals' basic rights and freedoms, and foster economic development and creativity in cyberspace. The EU's Cybersecurity Strategy, NIS Directive, GDPR, and ENISA are all critical tools for achieving these goals.

of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (7 February 2013) JOIN/2013/01 final.

62 Joint Communication to the European Parliament, *ibid*.

63 NIS 2 Directive (n 42).

64 *ibid*.

65 *ibid*.

66 *ibid*.

67 GDPR (n 41).

68 ENISA, 'About ENISA – The European Union Agency for Cybersecurity' (ENISA) <<https://www.enisa.europa.eu/about-enisa>> accessed 26 March 2023; Cybersecurity Act (n 51).

3.1.2 Organization of American States (OAS)

The OAS is a global organisation with 35 member countries from North, Central, and South America, as well as the Caribbean.⁶⁹ The Organization of American States has acknowledged the necessity of tackling cyberspace concerns and has launched a variety of initiatives and regulations to do so.

To address cybersecurity challenges in the Americas, the OAS has launched a number of programs and regulations. The Inter-American Committee against Terrorism (CICTE), for example, has been attempting to encourage member governments to cooperate to prevent and combat cybercrime.⁷⁰ Furthermore, the OAS has established the Inter-American Committee on Telecommunications (CITEL) Cybersecurity Program, which aims to support the development of national cybersecurity policies and regulations, as well as collaboration and information-sharing among Member States.⁷¹ The initiative also offers Member States technical help and cybersecurity training.

In addition to these initiatives and policies, the OAS has established the Cybersecurity Technical Assistance Missions, which provides technical assistance to Member States on a variety of cybersecurity issues, such as developing national cybersecurity strategies and implementing international cybersecurity standards.⁷²

Notwithstanding these efforts, the OAS has considerable obstacles in tackling cybersecurity threats throughout the Americas. One significant difficulty is the lack of a coordinated and unified strategy for cybersecurity among Member States, which can stymie effective collaboration and information exchange.⁷³ Moreover, increased awareness and capacity-building among Member States are required, notably in creating and executing national cybersecurity plans and regulations.

In conclusion, the OAS has developed a variety of initiatives and policies to address cybersecurity challenges in the Americas, including the formation of the CICTE and the passage of multiple cybercrime resolutions. Yet, the OAS has substantial obstacles in addressing cybersecurity concerns in the region,

69 OAS, 'Who We Are' (OAS) <www.oas.org/en/about/who_we_are.asp> accessed 20 March 2023; Editors of Encyclopaedia Britannica, 'Organization of American States' (Britannica, Last Update 12 February 2023) <www.britannica.com/topic/Organization-of-American-States> accessed 27 March 2023.

70 US Department of State, 'Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)' (US Department of State) <<https://2001-2009.state.gov/s/ct/intl/io/cicte/index.htm>> accessed 27 March 2023.

71 OAS, 'The Inter-American Telecommunication Commission' (OAS) <www.oas.org/ext/en/main/oas/our-structure/agencies-and-entities/citel> accessed 27 March 2023.

72 Cybil, Cybersecurity Technical Assistance Missions (Cybil) <<https://cybilportal.org/projects/cybersecurity-technical-assistance-missions/>> accessed 27 March 2023.

73 OAS, NCS: *Lessons Learned and Reflections from the Americas and Other Regions* (OAS) 12.

including the need for increased cooperation and capacity-building among member governments.

3.1.3 *Organization for Security and Cooperation in Europe (OSCE)*

The OSCE is a regional security organisation that has 57 Member States from North America, Europe, and Asia.⁷⁴ The organisation's goal is to improve regional security, stability, and collaboration by tackling a wide variety of security challenges, particularly those in cyberspace.⁷⁵

The OSCE acknowledges the rising importance of cyberspace as an arena for international cooperation and has established a number of policy documents and initiatives to address emerging cyberspace concerns.⁷⁶ The OSCE's approach to cyberspace, like the EU's, is founded on the principle of a free, open, and secure cyberspace.⁷⁷

The OSCE has accepted various cyberspace policy publications, notably the Tallinn Manual on International Law Applicable to Cyber Warfare, which was prepared in collaboration with NATO and several other organisations in 2013.⁷⁸ The guidebook presents a thorough examination of international law related to cyberspace, including armed conflict law, human rights law, and State responsibility law.⁷⁹ It is largely considered a reliable source of international law in cyberspace.

In addition to the Tallinn Manual, the OSCE has approved a number of other policy papers, notably the 2013 OSCE Confidence Building Measures (CBMs) to mitigate conflict risks associated with the use of information and communication technology.⁸⁰ CBMs involve frequent information exchanges,

74 OSCE, 'Participating States' (OSCE) <www.osce.org/participating-states> accessed 28 March 2023.

75 OSCE, 'Who we are' (OSCE) <www.osce.org/who-we-are> accessed 28 March 2023.

76 Alena Kupchyna, 'Confronting the Challenges of Working in Cyberspace' (OSCE, 4 October 2021) <<https://www.osce.org/blog/confronting-the-challenges-of-working-in-cyberspace>> accessed 28 March 2023.

77 *ibid.*

78 Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Operations* (CUP 2013).

79 *ibid.*

80 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection' (CCDCOE) <<https://ccdcoe.org/incyber-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/>> accessed 28 March 2023; OSCE Permanent Council, 'Decision No. 1039 Development of Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (26 April 2012) PC.DEC/1039.

discussions, and visits among participating governments, as well as the development of emergency communication channels.⁸¹

The OSCE has also created a variety of capacity-building projects to help member governments improve their cybersecurity capabilities. For example, the International Cyber Security Capacity Building Program offers member governments training and technical help in incident response, cybersecurity strategy, and cybersecurity risk assessment.⁸²

Overall, the OSCE's cyberspace legislation and policy framework is built on the idea of a free, open, and safe cyberspace. The group has created a comprehensive approach to cyberspace security that includes policy papers, confidence-building measures, and capacity-building activities. The OSCE's activities in this field contribute significantly to the establishment of international norms and standards for responsible state behaviour in cyberspace.

3.1.4 *Association of Southeast Asian Nations (ASEAN)*

After analysing the topic of international law in cyberspace, it leads to a smaller framework, namely the ASEAN Member States' framework. ASEAN is also a group of countries that profit from and are harmed by technological advancement. While not as visible as other regional countries, ASEAN has positioned itself to deal with dangers that may arise at any time. Consequently, this part will discuss ASEAN's broad legal and policy challenges, as well as notable cases from specific Member States. It will use three major countries as examples: Indonesia, Singapore, and Thailand. Indonesia and Singapore are ASEAN member nations that are specialists in the GGE and have long contributed to the research and development of the subject. While Thailand is not a member of any international bodies, it has some noteworthy policy initiatives that will be addressed in further depth later.

Through the principle of comprehensive security,⁸³ Article 1(8) of the ASEAN Charter mandates effective activities to address all types of threats, transnational crimes, and transboundary issues. This Article does not explicitly discuss catastrophes and actions performed in ASEAN cyberspace; rather, it covers all types of risks, including ICT threats.

In 1996, ASEAN, which had only seven Member States at the time, convened multiple meetings on internet possibilities and challenges.⁸⁴ A number of issues were discussed at the time to prepare citizens for digital collaborations

81 *ibid.*

82 ICT4Peace, 'International Cyber Security Capacity Building Program' (ICT4Peace, 27 August 2018) <<https://ict4peace.org/wp-content/uploads/2018/09/Outline-Capacity-Building-20180827.pdf>> accessed 28 March 2023.

83 ASEAN Charter, art 1 (8).

84 ASEAN Secretariat, *Joint Press Release of the ASEAN Forum on Internet, Singapore, 2-4 September 1996* (ASEAN Secretariat 1996).

such as the e-ASEAN framework agreement and information and communications technology (ICT) capacity building⁸⁵, responding to cybercrime issues⁸⁶, terrorist use of the internet⁸⁷, and disinformation and misinformation dissemination.⁸⁸

ASEAN, on the other hand, has not implemented any actual rules or regulations. However, it has been decided by the issuing of policies that are applicable to all ASEAN Members, particularly the 2020 ASEAN ICT Masterplan⁸⁹, the 2025 ASEAN Connectivity Master Plan⁹⁰, and the ASEAN Smart Cities Network.⁹¹ Furthermore, ASEAN has held a number of meetings on cyber issues at various levels, including the ASEAN Regional Forum, the ASEAN Defence Ministers' Meeting, the ASEAN Ministerial Meeting on Transnational Crime, the ASEAN Digital Ministers' Meeting, and the ASEAN Ministerial Conference on Cybersecurity.⁹²

More diplomatic sensitivities surrounding espionage will be explored within the ASEAN framework, highlighting political intent, legal ambiguity, and a lack of competence.⁹³

85 ASEAN Secretariat, 'e-ASEAN Framework Agreement' (ASEAN, 24 November 2000) <<https://agreement.asean.org/media/download/20140119121135.pdf>> accessed 28 March 2023; ASEAN Secretariat, 'Brunei Action Plan "Enhancing ICT Competitiveness: Capacity Building"' (ASEAN, 19 September 2006) <<https://asean.org/brunei-action-plan-enhancing-ict-competitiveness-capacity-building/>> accessed 28 March 2023.

86 ASEAN Secretariat, 'ASEAN Document Series on Transnational Crime: Terrorism and Violent Extremism; Drugs; Cybercrime; and Trafficking in Persons' (ASEAN Jakarta 2007) <<https://asean.org/wp-content/uploads/2021/01/ASEAN-Documents-on-Transnational-Crime-FINAL-with-link2.pdf>> accessed 28 March 2023.

87 ASEAN Secretariat, 'Chairman's Statement of the Thirteenth ASEAN Regional Forum Kuala Lumpur, 28 July 2006' (ASEAN, Kuala Lumpur, 28 July 2006) <<https://asean.org/chairmans-statement-of-the-thirteenth-asean-regional-forum-kuala-lumpur-28-july-2006/>> accessed 28 March 2023; ASEAN Secretariat, 'ASEAN Regional Forum (ARF) Statement on Preventing and Countering Terrorism and Violent Extremism Conductive to Terrorism (VECT)' (26th ASEAN Regional Forum, Bangkok, Thailand, 2 August 2019) <https://aseanregionalforum.asean.org/wp-content/uploads/2019/08/ARF-Statement-on-Counter-Terrorism-and-VECT_FINAL.pdf> accessed 28 March 2023.

88 See, for example, ASEAN Learning Center, Department of Local Administration, 'ASEAN Ministers Agree on Framework to Combat Fake News' (Department of Local Administration, 11 May 2018) <<https://asean.dla.go.th/>> accessed 28 March 2023.

89 ASEAN Secretariat, 'The ASEAN ICT Masterplan 2020' (ASEAN 2020) <https://asean.org/wp-content/uploads/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf> accessed 28 March 2023.

90 ASEAN Secretariat, 'Master Plan on ASEAN Connectivity 2025' (ASEAN 2016) <https://asean.org/wp-content/uploads/2021/08/8_compressed.pdf> accessed 28 March 2023.

91 ASEAN Smart Cities Network (ASCN), 'ASEAN Smart Cities Framework' (ASCN 2018) <<https://asean.org/wp-content/uploads/2019/02/ASCN-ASEAN-Smart-Cities-Framework.pdf>> accessed 28 March 2023.

92 Elina Noor, 'Positioning ASEAN in Cyberspace' (2020) 15 (2) Asia Policy 107, 109.

93 *ibid* 111.

To begin with, decisions on any cyber activity are frequently political in nature. It indicates that the discovered advanced persistent threats are merely a subset of Southeast Asia's overall threat landscape, and certain ASEAN Member States have been involved in comparable advanced persistent threat operations.⁹⁴ In this sense, ASEAN may have both regional and national interests to consider in building its framework. Political calculation frequently works against naming and shaming perpetrators.

On the second point, while the applicability of international law in cyberspace is widely agreed upon, the criteria and specifics remain unclear.⁹⁵ Therefore, further features must be determined by country or within the framework of the region. There is currently no clear rule for ASEAN on how to determine the limits.

Finally, if a cyber attack is an act that an ASEAN State's domestic law designates as a crime under its domestic law. This problem may not be explicitly expressed by all ASEAN Member States or may be addressed by differing responsibility scopes. As a result, the legal, technical, or judicial capability action should be specified.⁹⁶ These are still not expressed directly in the ASEAN framework.

3.2 Examples from some countries

Since the employment of cyberspace has grown in popularity in modern society, several States have enacted domestic rules and regulations to regulate the activities that occur within it. The Computer Misuse Act of 1990,⁹⁷ for example, criminalises unauthorised access to computer systems and associated offences in the United Kingdom. Similarly, Germany passed the Federal Office for Information Security Act,⁹⁸ which sets steps to safeguard the security and resilience of government information technology systems. France has enacted the Military Planning Law,⁹⁹ which improves cyber defences and enables

94 Jason Thomas, 'Cyber warfare in Vietnam' (*The ASEAN Post*, 4 October 2019) <<https://theaseanpost.com/article/cyber-warfare-vietnam>> accessed 28 March 2023.

95 GGE 2021 Report (n 1).

96 International Telecommunication Union (ITU), 'Global Cybersecurity Index 2020' (ITU Publications 2020) <www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf> accessed 28 March 2023.

97 Computer Misuse Act (n 46).

98 Act on the Federal Office for Information Security (BSI Act - BSIG), BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821).

99 Cours des comptes, 'The French Military Programming Law (LPM) 2019-2025 and the Capacities of the Armed Forces' (Press Release, 11 May 2022) <<https://www.ccomptes.fr/system/files/2022-07/20220511-press-release-The-French-military-programming-law-2019-2025-and-capacities-of-armed-forces.pdf>> accessed 28 March 2023.

offensive cyber responses to certain threats. The Information Society Code¹⁰⁰ governs electronic communications in Finland, whereas the Computer Misuse and Cybersecurity Act¹⁰¹ in Singapore forbids illegal access and calls for the development of a national cybersecurity agency. These instances demonstrate the numerous ways in which countries use domestic legislation to handle cyberspace challenges.

3.2.1 *The United Kingdom*

The United Kingdom has established an extensive legal and policy framework to cover various areas of cyberspace. The framework is made up of both domestic laws and international treaties. In addition, the UK government has released a number of policies and measures to improve its cybersecurity posture and preserve its national interests.

Domestically, the United Kingdom has enacted a number of laws and regulations to combat cybercrime, cyber assaults, and data protection. The Computer Misuse Act 1990¹⁰² criminalises illegal access to computer systems, while the Police and Justice Act 2006¹⁰³ makes it an offence to initiate a cyber assault that results in the interruption of services. Moreover, the Data Protection Act 2018¹⁰⁴ brings the EU GDPR¹⁰⁵ into the United Kingdom and establishes principles for the processing and protection of personal data.

The UK government has also established a number of organisations and entities to guarantee that these laws are implemented and enforced. The National Cyber Security Centre (NCSC),¹⁰⁶ which is part of the Government Communications Headquarters (GCHQ), is responsible for identifying and mitigating cyber threats in the United Kingdom. The NCSC also advises and assists organisations and individuals in improving their cybersecurity posture.¹⁰⁷

At the international level, the United Kingdom is a signatory to many cybersecurity treaties, including the Budapest Convention on Cybercrime¹⁰⁸ and the

100 Ministry of Transport and Communication, Act on Electronic Communications Services (917/2014; amendments up to 1207/2020 included) (translation from Finnish) <<https://www.finlex.fi>> accessed 29 March 2023.

101 Computer Misuse and Cybersecurity (Amendment) Act 2017 (No 22 of 2017), Government Gazette Acts Supplement (12 May 2017).

102 Computer Misuse Act (n 46).

103 Police and Justice Act 2006, UK Public General Act 2006, c.48.

104 Data Protection Act 2018 (n 47).

105 Please note that even though the UK has leaved the EU and all EU regulations shall not be applied to the UK, the UK has legalised the GDPR in its Data Protection Act 2018, resulting that the GDPR substances are still applied to the UK jurisdiction.

106 National Cyber Security Centre, 'What We Do' (NCSC) <<https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>> accessed 29 March 2023.

107 *ibid.*

108 Budapest Convention (n 8).

NATO Coordinated Cyber Defence Centre of Excellence (CCDCOE).¹⁰⁹ The United Kingdom also takes part in a number of international forums and conferences to address cybersecurity challenges and share best practices.

In addition to these legal and legislative frameworks, the United Kingdom has created a number of policies and efforts to strengthen its security strategy. The National Cyber Security Strategy 2022-2030 outlines the UK government's strategy and goals for cybersecurity in the country.¹¹⁰ Among the elements in the strategy are investments in cybersecurity research and development, boosting the country's cyber defences, and enhancing international collaboration.

Overall, the United Kingdom's legal and legislative framework for cyberspace is extensive, reflecting the country's commitment to defending its national interests and preserving citizens' security. Yet, because cybersecurity threats are continually developing, the UK government must continue to examine and adapt its policies and plans in order to keep ahead of emerging risks and difficulties.

3.2.2 *Germany*

To meet the difficulties posed by cyberspace, Germany has built a comprehensive legal and policy framework. The country has taken several initiatives to defend its critical infrastructure and prevent cybercrime, while also emphasising the need for international collaboration in dealing with cybersecurity challenges.

The IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0),¹¹¹ enacted in 2021, is an important legal instrument in Germany's cyber strategy. The Act compels firms that operate vital infrastructure to take specific cybersecurity measures and to notify the Federal Office for Information Security of any serious cybersecurity incidents (BSI).¹¹² The Act also established the BSI as Germany's national authority for information security, in charge of coordinating the country's cybersecurity activities as well as offering guidance and help to businesses and people.

Germany has also taken initiatives to prevent cybercrime, such as passing the Act to Improve the Enforcement of Criminal Law in Cyberspace (Gesetz zur Verbesserung der Durchsetzung von Rechten im Cyberspace) in 2017.¹¹³ The

109 CCDCOE, 'About Us' (CCDCOE) <<https://ccdcOE.org/about-us/>> accessed 29 March 2023.

110 HM Government, 'Government Cyber Security Strategy: Building a cyber resilient public sector 2022-2030' (HM Government) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf> accessed 29 March 2023, 18–27.

111 Federal Office for Information Security, 'Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)' (Translation version) (BSI, 2021) <https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html> accessed 29 March 2023.

112 *ibid.*

113 Sandra Schmitz and Christian M Berndt, 'The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?' (Working Paper, 2019) <<https://papers.ssrn.com>>

Act criminalises a variety of cyber crimes, including hacking, cyber espionage, and malware creation and dissemination.¹¹⁴

In addition to these domestic measures, Germany has been an active participant in international efforts to improve cybersecurity. The government has been a significant supporter of the creation of international norms and guidelines for responsible cyberspace behaviour and has backed projects such as the Tallinn Manual on International Law Applicable to Cyber Warfare¹¹⁵ and the Global Commission on Cyberspace Stability.¹¹⁶

Germany's cybersecurity law and regulatory framework is broad and aggressive, with a heavy emphasis on protecting vital infrastructure and combatting cybercrime as can be seen from its position paper on cyberspace.¹¹⁷ The country's emphasis on international collaboration and the formation of standards and guidelines for responsible cyberspace behaviour indicates its appreciation of the importance of a coordinated and collaborative approach to resolving the issues posed by the digital age.

3.2.3 *France*

France has been working hard to build and execute legal and legislative frameworks to combat cyber threats. The government acknowledges that cyberspace poses a significant threat to national security and has made efforts to strengthen its legal and institutional capacities to address cyber threats.

France has enacted a number of rules and regulations to protect its critical infrastructure and combat cybercrime on a national level. For example, the National Cybersecurity Agency (ANSSI) was formed under the 2013 Military Programming Law (LPM) to manage the country's cybersecurity activities.¹¹⁸ ANSSI has been crucial in defining critical infrastructure regulations and standards, as well as offering advice to government agencies and the private sector.

France passed a new cybersecurity and data protection and privacy law in 2018, with the goal of improving the country's ability to prevent, detect, and

com/sol3/papers.cfm?abstract_id=3306964> (accessed 29 March 2023) 1–41; Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (G-SIG: 16019378), Federal Law Gazette I, XVI/343.

114 Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, *ibid*.

115 Schmitt (n 78).

116 Hague Centre for Strategic Studies (HCSS), 'Global Commission on the Stability of Cyberspace (GCSC)' (HCSS) <<https://hcss.nl/global-commission-on-the-stability-of-cyberspace-homepage/>> accessed 29 March 2023.

117 The German Federal Foreign Office and the German Federal Ministry of Defence, 'On the Application of International Law in Cyberspace' (German position paper, March 2021) <<https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>> accessed 30 March 2023.

118 National Cybersecurity Agency of France (ANSSI), 'The National Cybersecurity Agency of France' (SSI) <<https://www.ssi.gouv.fr>> accessed 30 March 2023.

respond to cyber threats.¹¹⁹ The law compels critical infrastructure operators to implement network security measures and to report cyber events to ANSSI. The law also gives ANSSI the authority to perform vulnerability assessments, monitor network traffic, and intervene to prevent cyber assaults.¹²⁰

France has formed various international partnerships to combat cyber risks in addition to its legal and regulatory framework. The country is a member of the European Union's Cybersecurity Agency (ENISA)¹²¹ and NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE),¹²² and it has taken part in a number of international cybersecurity efforts.

Notwithstanding these efforts, however, France continues to confront substantial challenges in coping with the expanding cyber threat scenario. Some high-profile cyber assaults have occurred in the nation, notably the 2017 WannaCry ransomware outbreak, which damaged thousands of systems globally.¹²³ France must continue to strengthen its legal and institutional skills in order to handle these concerns, notably by encouraging international collaboration and information exchange.

Finally, France has made tremendous progress in building and implementing its cyberspace legal and policy frameworks as appeared in the open-ended working group paper.¹²⁴ The government recognises the importance of cybersecurity to national security and has made initiatives to improve its response capabilities to cyber attacks. To meet the expanding cyber threat scenario, the government must stay attentive and continue to modify its legislative and institutional structures.

3.2.4 Finland

To address cybersecurity challenges, Finland has built a comprehensive legislative and policy framework. The country's approach to cybersecurity is a mix of domestic regulation, international collaboration, and public-private

119 Anne-Laure Villedieu, 'Data Protection and Cybersecurity Laws in France' (CMS, 2021) <<https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cybersecurity-laws/france>> accessed 30 March 2023; LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, 10 May 2018, INTX1728622L.

120 Villedieu, *ibid*.

121 ENISA (n 68).

122 CCDCOE (n 109).

123 Kaspersky, 'What is WannaCry Ransomware?' (Kaspersky) <<https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>> accessed 31 March 2023; RFI, 'French Researchers Crack Open WannaCry Ransomware' (RFI, 20 May 2017) <<https://www.rfi.fr/en/france/20170520-french-researchers-crack-open-wannacry-ransomware>> accessed 31 March 2023.

124 France, 'International law applied to operations in cyberspace' (Open-ended working group, December 2021) <<https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf>> accessed 31 March 2023.

partnerships. Finland has also been an active promoter of international cybersecurity rules and standards.

On a national level, Finland has adopted a number of cybersecurity legislation and regulations. The most important of them is the Act on the Protection of Privacy in Electronic Communications, which regulates personal data processing and electronic communication secrecy.¹²⁵ The Information Security Act,¹²⁶ the Criminal Code,¹²⁷ and the Data Protection Act¹²⁸ are all significant statutes. These laws offer the legal foundation for maintaining critical infrastructure security and punishing cyber criminals.

Finland has a cyber security strategy, which was initially published in 2013 and was recently revised.¹²⁹ The plan specifies the country's cybersecurity goals and objectives, such as improving the cybersecurity skills of government agencies, critical infrastructure operators, and other stakeholders. In addition, the policy emphasises the necessity of international cooperation in solving cybersecurity concerns.

Finland is also an active participant in worldwide cybersecurity activities in addition to its national efforts. Since its founding in 2014, Finland has been a member of the EU's Network and Information Security Cooperation Group (ENISA),¹³⁰ as well as a member of the NATO CCDCOE.¹³¹ Finland has also been a key contributor to the establishment of international cybersecurity rules and standards, such as the Tallinn Manual on International Law Applicable to Cyber Warfare¹³² and the Paris Call for Trust and Security in Cyberspace.¹³³

Generally, Finland's cybersecurity law and policy framework is extensive and well-developed. This includes its national positions dealing with cyber threats.¹³⁴ To meet the complex and developing difficulties of cyberspace, the country's

125 Act on the Protection of Privacy in Electronic Communications (516/2004; amendments up to 365/2011 included) (Unofficial Translation) <<https://www.finlex.fi>> accessed 31 March 2023; DLA Piper, *Data Protection Laws of the World: Finland* (DLA Piper) 1–16.

126 Government Decree on Information security in central government (681/2010) (Unofficial Translation) <<https://https://finlex.fi/en>> accessed 31 March 2023.

127 Finland Penal Code, Chapter 38, section 8.

128 Jukka Lang and Tuomas Haavikko, 'Data Security and Cybercrime in Finland' (Lexology, 14 January 2019) <<https://www.lexology.com/library/detail.aspx?g=9d-2dd419-3a42-464a-8df0-ed1ffb9dedd7>> accessed 31 March 2023.

129 Ministry of Foreign Affairs of Finland, 'Cyber security and the cyber domain' (Ministry of Foreign Affairs) <<https://um.fi/cyber-security-and-the-cyber-domain>> accessed 31 March 2023.

130 ENISA (n 68).

131 CCECOE (n 122).

132 Schmitt (n 78).

133 Paris Call for Trust and Security in Cyberspace <<https://pariscall.international/en/call>> accessed 31 March 2023.

134 Finland (n 25).

approach to cybersecurity incorporates national law, international collaboration, and public-private partnerships.

3.2.5 *Singapore*

Singapore is a leader in the implementation of international law in cyberspace. As Singapore presided over ASEAN in 2018, a framework for the ASEAN Cyber Capacity Program was formed,¹³⁵ as was the ASEAN Ministerial Conference on Cybersecurity,¹³⁶ which included the formation of the ASEAN-Singapore Cyber Center of Excellence.¹³⁷ The Centre's goal is to provide training, research, and information sharing on strategic, policy, legal, and operational cyberspace concerns. These initiatives are intended to integrate cyber diplomacy efforts with operational challenges in order to achieve regional collaboration toward a single stance on international platforms.¹³⁸ Australia, Canada, the European Union, South Korea, New Zealand, and the United Kingdom all contribute to the Centre's activities.¹³⁹

Singapore's stance on the application of international law in cyberspace is clearer than that of the other ASEAN members. Singapore contemplates dealing with cyberspace regulations, particularly during the State action in international law is critical in ensuring an open, safe, stable, accessible, peaceful, and interoperable ICT environment for digitalisation.¹⁴⁰ Singapore has said unequivocally that the laws regulating cyberspace under international law are governed by the United Nations Charter.¹⁴¹ Singapore has also said unequivocally that State sovereignty is a principle that applies equally to States. Other common law concepts of international law, such as the prohibition of interference, peaceful resolution of conflicts, self-defence, armed attack, and use of force, can also apply to cyber concerns. It is a basic value enshrined in the United Nations Charter.¹⁴² Other principles may also be implemented to the extent practicable. It is critical to evaluate the consequences of cyber activity. Malicious cyber activity

135 International Telecommunication Union (ITU), 'Global Cybersecurity Index 2020' (ITU Publications 2020) <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf> accessed 1 April 2023.

136 ASEAN Secretariat (n 12).

137 Cyber Security Agency of Singapore (n 32).

138 Government of Singapore (n 60).

139 Noor (n 92) 113.

140 United Nations, 'Singapore's Views on Developments in the Field of Information and Telecommunications in the Context of International Security, Pursuant to General Assembly Resolutions 73/27 and 73/266' (UN 2019) <<https://www.un.org/en/>> accessed 1 April 2023.

141 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'National position of Singapore (2021)' (CCDCOE, 25 November 2021) <[https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_\(2021\)](https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_(2021))> accessed 1 April 2023; United Nations General Assembly (n 178) para 83.

142 CCECOE, *ibid*; UN General Assembly, *ibid* paras 83–84.

attributable to a State, for example, that interferes with the normal governing functions of a victim State is an example of an internationally unlawful act.¹⁴³

4. Applicability of regional and domestic legal instruments and policy framework in cyberspace

Cyberspace is a complicated and rapidly evolving domain that presents various legal issues. These challenges include personal data security, cyber behaviour regulation, and cybercrime prevention. Several legal tools and policy frameworks have been established at the international, regional, and national levels to tackle these issues.

Regional organisations have also established legal tools and policy frameworks to handle legal challenges in cyberspace. The Convention on Cybercrime of the Council of Europe,¹⁴⁴ for example, is a regional legislative framework that strives to improve cybersecurity and safeguard personal data in their respective regions.

Some States have built their legal frameworks and strategies to address cyberspace legal challenges on a domestic basis.¹⁴⁵ Legislation that criminalises cybercrime, regulates online activity, and safeguards personal data is included in these frameworks. Local legislative frameworks also provide tools for international collaboration in the fight against cyber threats and the promotion of cybersecurity.

In this regard, the unique nature of cyberspace, as well as its implications for issues of State sovereignty, extraterritoriality, and the idea of cyberspace sovereignty, are obstacles to the application of international law principles. The numerous legal difficulties that exist in cyberspace are discussed here, as well as how international law might be used to overcome them.

143 United Nations General Assembly, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law applies to the Use of Information and Communications Technologies by States submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136, para 84.

144 Budapest Convention (n 8).

145 See, for example, Foreign, Commonwealth & Development Office (n 45); German Federal Foreign Office and the German Federal Ministry of Defence (n 117); France (n 124); Finland (n 25).

4.1 Regional and domestic legal instruments and policy framework to State sovereignty violation

4.1.1 Regional level

Regional legal instruments and policy frameworks play an important role in dealing with abuses of state sovereignty in cyberspace. To solve these problems, some regional organisations have adopted legal tools and policy frameworks. The EU, the OAS, the OSCE, and the ASEAN and their approaches to state sovereignty violations in cyberspace will be examined in this research.

The EU's approach to state sovereignty violations in cyberspace is founded on the principles of state sovereignty, territorial integrity, and critical infrastructure protection. The EU's Cybersecurity Strategy highlights the necessity of protecting critical infrastructure from cyber attacks while also encouraging collaboration among member states and private sector stakeholders.¹⁴⁶ The EU also backs international initiatives to encourage responsible state behaviour in cyberspace, such as the creation of rules and confidence-building measures.¹⁴⁷ The EU's efforts in this area have resulted in the creation of legislative instruments such as the EU Cybersecurity Act¹⁴⁸ and the NIS2 Directive,¹⁴⁹ which aim to improve cybersecurity and protect the EU's critical infrastructure.

The OAS's approach to state sovereignty violations in cyberspace is based on the principles of non-intervention and human rights protection. The OAS has created the Inter-American Convention Against Cybercrime, which criminalises cyber actions such as hacking, cyber fraud, and the distribution of dangerous software.¹⁵⁰ The Convention also establishes a framework for international co-operation in cybercrime investigation and prosecution. Furthermore, the OAS encourages the development of cybersecurity capabilities in its Member States, including the formulation of national cybersecurity policies and the adoption of international standards.

The OSCE's approach to State sovereignty violations in cyberspace is guided by principles of human rights, basic freedoms, and the rule of law. The OSCE's cyber/ICT security Concept emphasises the necessity of safeguarding critical infrastructure and encouraging international collaboration in combating cyber threats.¹⁵¹ The OSCE also fosters the development of confidence-build-

146 Vela (n 61); Joint Communication to the European Parliament (n 61).

147 CCDCOE (n 80).

148 Cybersecurity Act (n 51).

149 NIS 2 Directive (n 42).

150 US Department of State (n 70).

151 CCDCOE (n 80); OSCE Permanent Council (n 80); OSCE Permanent Council, 'Decision No. 1202 OSCE Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202.

ing measures¹⁵² and the adoption of rules for responsible state behaviour in cyberspace. In addition, the OSCE has launched a variety of capacity-building projects to assist its Member States in improving their cybersecurity capabilities.

The ASEAN approach to state sovereignty violations in cyberspace is built on the principles of non-intervention and respect for country sovereignty. ASEAN has established the ASEAN Regional Forum Declaration on Cooperation in the Area of Information and Communication Technology (ICT) Security, which underlines the necessity of member-state collaboration in dealing with cyber threats.¹⁵³ ASEAN also encourages the establishment of capacity-building programs and the implementation of international cybersecurity rules and standards.¹⁵⁴

In conclusion, regional legal instruments and policy frameworks play an important role in resolving violations of state sovereignty in cyberspace. Various regional organisations have produced legal instruments and policy frameworks that reflect their particular regional environments and agendas. The EU, OAS, OSCE, and ASEAN all have various ways of dealing with state sovereignty violations in cyberspace, but they all have the same aim of improving cybersecurity and preserving critical infrastructure.

4.1.2 Domestic level

Domestic legal instruments and policy frameworks are also important in dealing with state sovereignty violations in cyberspace. To address these issues, some countries have established legal instruments and policy frameworks. This analysis will examine the approaches of the UK, Germany, France, Finland, and Singapore to State sovereignty violations in cyberspace.

The UK's approach to State sovereignty violations in cyberspace is based on the concepts of national security and critical infrastructure protection. The United Kingdom's National Cyber Security Strategy establishes a comprehensive strategy for cybersecurity, including efforts to safeguard critical infrastructure, improve intelligence capabilities, and foster international collaboration.¹⁵⁵ The UK has also passed the Cybersecurity Information Sharing Act, which establishes a legal framework for the exchange of cybersecurity data between public and private sector institutions.¹⁵⁶

152 CCDCOE, *ibid*.

153 ASEAN Secretariat (n 86); ASEAN Secretariat (n 87); ASEAN Secretariat (n 89).

154 Government of Singapore (n 60); Nur Azha Putra (n 60).

155 National Cyber Security Centre (n 106).

156 Foreign & Commonwealth Office, 'Guidance on Cyber-threat intelligence information sharing guide' (GOV.UK, 8 March 2021) <www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide> accessed 3 April 2023.

Germany's approach to State sovereignty violations in cyberspace is grounded in the principles of human rights and critical infrastructure protection. To counter cyber risks, the German government has created a variety of legislative instruments, including the Cybersecurity Act¹⁵⁷ and the IT Security Act.¹⁵⁸

France's approach to State sovereignty violations in cyberspace is based on the concepts of national security and critical infrastructure protection. The French government has created a variety of legislative tools to combat cyber risks, including the Military Programming Law¹⁵⁹ and the National Cybersecurity Strategy.¹⁶⁰

Finland's approach to State sovereignty violations in cyberspace is built on the principles of human rights and critical infrastructure protection. To counter cyber risks, the Finnish government has created a variety of legislative instruments, including the Act on the Protection of Privacy in Electronic Communications¹⁶¹ and the Cybersecurity Strategy.¹⁶²

Singapore's approach to State sovereignty violations in cyberspace is based on national security and critical infrastructure protection principles. The Singapore government has created a variety of legislative tools to combat cyber threats, including the Cybersecurity Bill which later becomes the Cybersecurity Act.¹⁶³

In conclusion, domestic legal instruments and policy frameworks are crucial for dealing with violations of State sovereignty in cyberspace. Many States have created legal instruments and policy frameworks that reflect their situations and agendas. The approaches employed by the UK, Germany, France, Finland, and Singapore to resolve State sovereignty violations in cyberspace vary, but they all have the same aim of boosting cybersecurity and preserving key infrastructure. These laws aim to strengthen cybersecurity and protect critical infrastructure by introducing clear cybersecurity standards for corporations and government agencies.

157 Sandra Schmitz and Christian M Berndt (n 113) 1–41; Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (G-SIG: 16019378) (n 113).

158 Federal Office for Information Security, 'Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)' (Translation version) (BSI, 2021) <www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html> accessed 3 April 2023.

159 Cours des comptes (n 99).

160 National Cybersecurity Agency of France (ANSSI) (n 118).

161 Act on the Protection of Privacy in Electronic Communications (516/2004; amendments up to 365/2011 included) (n 125).

162 Ministry of Foreign Affairs of Finland, 'Cyber security and the cyber domain' (Ministry of Foreign Affairs) <<https://um.fi/cyber-security-and-the-cyber-domain>> accessed 4 April 2023.

163 Singapore Government Agency, 'Cybersecurity Act' (Cyber Security Agency of Singapore) <<https://www.csa.gov.sg/legislation/Cybersecurity-Act>> accessed 2 March 2023.

4.2 Regional and domestic legal instruments and policy framework for extraterritorial effects

4.2.1 *Regional level*

Regional legal instruments and policy frameworks play a significant role in tackling extraterritorial effects in cyberspace. The potential of activities made in one state to have an influence on another is referred to as extraterritoriality. This might result in complicated legal challenges requiring international collaboration and coordination. The purpose of this part is to look at how the EU, the OAS, the OSCE, and the ASEAN deal with extraterritoriality in cyberspace.

The EU has created a comprehensive framework for dealing with extraterritoriality in cyberspace. The EU's GDPR applies to all companies, regardless of location, that process the personal data of EU citizens.¹⁶⁴ This implies that companies operating outside the EU must follow EU data protection standards if they process EU citizens' data. The GDPR also includes the right to be forgotten, which permits individuals to request that their personal data be deleted from online platforms situated outside of the EU.¹⁶⁵ In addition, the EU has a number of bilateral and multilateral agreements with other States in place to enhance international collaboration and coordination on cybersecurity issues.¹⁶⁶

The OAS has developed a variety of legislative instruments to address extraterritoriality in cyberspace. The Inter-American Cooperation Portal on Cyber-Crime establishes a framework for collaboration among OAS Member States in cybercrime investigation and prosecution.¹⁶⁷ The OAS also runs a Cybersecurity Program, which offers Member States technical support to help them enhance their cybersecurity capabilities.¹⁶⁸

The OSCE has established an extensive strategy for dealing with extraterritoriality in cyberspace. The OSCE's Confidence-Building Measures (CBMs) in Information and Communication Technology seek to improve openness and collaboration among OSCE member states on cybersecurity problems.¹⁶⁹ The OSCE also operates a Cybersecurity Capacity Building Program, which offers Member States training to assist them to strengthen their cyberspace competency.¹⁷⁰

164 GDPR (n 41).

165 GDPR, *ibid* art 17; Ben Wolford, 'Everything You Need to Know about the "Right to be Forgotten"' (GDPR) <<https://gdpr.eu/right-to-be-forgotten/>> accessed 4 April 2023.

166 NIS 2 Directive (n 42); Cybersecurity Act (n 51); Jorida Vela (n 61); Joint Communication to the European Parliament (n 61).

167 OAS, 'The Inter-American Cooperation Portal on Cyber-Crime' (Cybercrimedata AS) <<https://www.cybercrimelaw.net/OAS.html>> accessed 5 April 2023.

168 US Department of State (n 70).

169 CCDCOE (n 80); OSCE Permanent Council (n 80).

170 ICT4Peace (n 82).

ASEAN has set up a number of legal mechanisms to deal with extraterritoriality in cyberspace. The e-ASEAN framework agreement and information and communications technology (ICT) capacity building establishes a framework for ASEAN member states to collaborate on cybersecurity challenges.¹⁷¹ The ASEAN Cybersecurity Cooperation Strategy also includes a road map for improving regional cybersecurity cooperation and coordination.¹⁷²

In conclusion, regional legal instruments and policy frameworks are important in tackling extraterritoriality in cyberspace. The EU, OAS, OSCE, and ASEAN all take various approaches to these concerns, but they all share the objective of strengthening international collaboration and coordination on cybersecurity issues. These regional frameworks are critical for dealing with the complex legal challenges that arise in cyberspace and maintaining a safe and secure digital environment for all.

4.2.2 *Domestic level*

Domestic legal instruments and policy frameworks are equally significant in dealing with extraterritoriality in cyberspace. This analysis looks at how the UK, Germany, France, Finland, and Singapore approach extraterritoriality in cyberspace through domestic legal instruments and policy frameworks.

The UK has taken several measures to address extraterritoriality in cyberspace. The Data Protection Act 2018 of the UK applies to all companies that process the personal data of UK citizens, regardless of where they are located.¹⁷³ This means companies operating outside of the UK must follow UK data protection legislation if they process data from UK residents. In addition, the UK has a variety of regulations in place to combat cybercrime, notably the Computer Misuse Act of 1990¹⁷⁴ and the Police and Justice Act of 2006.¹⁷⁵

Germany has also taken measures to combat extraterritoriality in cyberspace. The German Federal Data Protection Act applies to all enterprises, wherever they occur, that process the personal data of German residents.¹⁷⁶ The Act also includes a right-to-be-forgotten provision, which allows individuals to request that their personal data be deleted from online platforms situated outside of Germany.¹⁷⁷ Germany recently approved the Network Enforcement Act, which

171 ASEAN Secretariat (n 86).

172 ASEAN Secretariat (n 12).

173 Data Protection Act 2018 (n 47).

174 Computer Misuse Act (n 46).

175 Police and Justice Act 2006 (n 103).

176 Federal Data Protection Act (BDSG) (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

177 Didomi, 'Germany's data privacy protection laws: Everything you need to know' (Didomi, 26 February 2023) <<https://blog.didomi.io/en/germany-data-privacy-protection-laws-everything-you-need-to-know>> accessed 6 April 2023.

mandates that social media firms remove illegal content within 24 hours or face fines.¹⁷⁸

France has implemented a number of efforts to combat extraterritoriality in cyberspace. The French Data Protection Act applies to all enterprises, regardless of geography, that process the personal data of French citizens.¹⁷⁹ France recently ratified the Military Programming Law 2019-2025, which contains steps to strengthen the country's cybersecurity capabilities and battle cyber threats.¹⁸⁰

Under its Cyber Security Strategy, Finland has put in place measures aimed at combating extraterritoriality in cyberspace.¹⁸¹ The Strategy establishes a framework for improving cybersecurity cooperation and coordination among Finland and other States. Finland has also approved the Data Protection Act, which applies to all enterprises, irrespective of where they operate, that process the personal data of Finnish citizens.¹⁸²

Through its Cybersecurity Act, Singapore has put in place safeguards to counter extraterritorial effects in cyberspace.¹⁸³ The Act requires key information infrastructure owners to implement cybersecurity safeguards for their systems and regulates cybersecurity service providers.¹⁸⁴ Singapore has also set up a Cyber Security Agency, which is in charge of coordinating cybersecurity operations and responding to cyber attacks.¹⁸⁵

Consequently, domestic legal instruments and policy frameworks are critical in tackling extraterritoriality in cyberspace. The United Kingdom, Germany, France, Finland, and Singapore all take various approaches to these concerns, but they all share the objective of ensuring a safe and secure digital environment for their inhabitants. These domestic frameworks are critical for handling the complex legal challenges that occur in cyberspace, as well as for encouraging international collaboration and coordination on cybersecurity matters.

178 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech' (Library of Congress, 2021) <www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/> accessed 6 April 2023.

179 OneTrust DataGuidance, 'The Data Protection Act' (DataGuidance) <www.dataguidance.com/sites/default/files/france_data_protection_act.pdf> accessed 6 April 2023.

180 ANSSI (n 118).

181 Ministry of Foreign Affairs of Finland (n 162).

182 Lang, Haavikko (n 128).

183 Singapore Government Agency, 'Cybersecurity Act' (Cyber Security Agency of Singapore) <<https://www.csa.gov.sg/legislation/Cybersecurity-Act>> accessed 6 April 2023.

184 *ibid.*

185 Singapore Government Agency, 'Who We Are' (CSA) <<http://www.csa.gov.sg>> accessed 6 April 2023.

4.3 Regional and domestic legal instruments and policy framework for cyberspace sovereignty

4.3.1 Regional level

Regional legal instruments and policy frameworks are critical in resolving the challenges of cyberspace sovereignty. This examination will look at how the EU, the OAS, the OSCE, and the ASEAN deal with these issues.

The EU has implemented several measures to address cyberspace sovereignty issues. The EU Cybersecurity Act, passed in 2019, creates a European cybersecurity certification system with the goal of improving the cybersecurity of goods, processes, and services.¹⁸⁶ In addition, the EU has adopted a variety of laws and efforts to support the free movement of data inside the EU while protecting personal data and other rights. Furthermore, the EU has formed the ENISA, which provides cybersecurity advice and support to EU member states.¹⁸⁷

The OAS has also taken measures to deal with concerns about cyberspace sovereignty. The OAS has adopted a variety of cybersecurity resolutions, including the Inter-American Cybersecurity Strategy¹⁸⁸ and the Declaration on the Protection of Critical Infrastructure from Emerging Threats.¹⁸⁹ The OAS has also formed the CICTE, which encourages member governments to work together to combat cyberspace risks.¹⁹⁰

The OSCE has put in place a number of measures to address cyberspace sovereignty challenges. The OSCE has established a variety of CBMs targeted at increasing openness and lowering the danger of cyber warfare.¹⁹¹ The OSCE also encourages conversation and collaboration among Member States on cybersecurity problems through its annual Confidence-Building Measures Conference and its informal cybersecurity expert group.¹⁹²

ASEAN has made initiatives to resolve cyberspace sovereignty challenges through its 2020 ASEAN ICT Masterplan.¹⁹³ The Plan contains initiatives targeted at improving cybersecurity cooperation among ASEAN Member

186 Cybersecurity Act (n 51).

187 ENISA (n 68).

188 OAS, 'A comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity' (OAS) <http://www.oas.org/juridico/english/cyb_pry_strategy.pdf> accessed 7 April 2023.

189 Inter-American Committee Against Terrorism (CICTE), 'Declaration on the Protection of Critical Infrastructure from Emerging Threats' (23 March 2015) OEA/Ser.L/X.2.15, CICTE/doc.1/15.

190 US Department of State (n 70).

191 CCDCOE (n 80); OSCE Permanent Council (n 80); OSCE Permanent Council (n 151).

192 OSCE, 'Confidence and Security Building Measures' (OCSE) <<https://www.osce.org/secretariat/107484>> accessed 8 April 2023.

193 ASEAN Secretariat (n 89).

States and fostering the establishment of a secure and resilient digital environment.¹⁹⁴ ASEAN has also established the ASEAN Ministerial Conference on Cybersecurity, which provides a forum for Member States to debate cybersecurity challenges and foster collaboration.¹⁹⁵

In conclusion, regional legal instruments and policy frameworks are essential for tackling cyberspace sovereignty challenges. The EU, OAS, OSCE, and ASEAN all take various approaches to these concerns, but they all share the objective of creating a safe and secure digital environment for their inhabitants. These regional frameworks are critical for encouraging international collaboration and coordination on cybersecurity challenges, as well as resolving the complex legal issues that develop in cyberspace.

4.3.2 *Domestic level*

Domestic legal instruments and policy frameworks also play an important role in resolving cyberspace sovereignty challenges. In this part, they include the analysis of the UK, Germany, France, Finland, and Singapore dealing with cyberspace sovereignty challenges.

The UK has implemented a lot of measures to address cyberspace sovereignty concerns. The National Cyber Security Strategy of the UK seeks to make the country a safe and resilient digital nation.¹⁹⁶ The policy includes safeguards for important national infrastructure, increased cybersecurity skills and awareness, and collaboration with foreign partners to combat cyber attacks.¹⁹⁷ The United Kingdom has also established the National Cyber Security Centre (NCSC), which provides cybersecurity advice to organisations and individuals.¹⁹⁸

Germany has also begun addressing the problems of cyberspace sovereignty. Germany's cybersecurity plan includes efforts to protect key infrastructure, encourage cybersecurity research and development, and strengthen international cybersecurity cooperation.¹⁹⁹ The German government has also formed the Federal Office for Information Security (BSI), which is in charge of guaranteeing the security of government and critical infrastructure operators' information technology systems.²⁰⁰

Through its National Strategy for Cybersecurity, France has adopted measures to address the challenges of cyberspace sovereignty. The policy includes initiatives to improve critical infrastructure cybersecurity, encourage cybersecurity research and development, and strengthen international cybersecurity

¹⁹⁴ *ibid.*

¹⁹⁵ Government of Singapore (n 60); Nur Azha Putra (n 60).

¹⁹⁶ HM Government (n 110).

¹⁹⁷ *ibid.*

¹⁹⁸ National Cyber Security Centre (n 106).

¹⁹⁹ German Federal Foreign Office and the German Federal Ministry of Defence (n 117).

²⁰⁰ Federal Office for Information Security (n 158).

cooperation.²⁰¹ In addition, the French government formed the ANSSI, which is in charge of defending the government and critical infrastructure networks.²⁰²

Finland has implemented measures to address issues related to cyberspace sovereignty through its National Cyber Security Strategy.²⁰³ The policy includes efforts to secure key infrastructure, strengthen Finnish organisations' and people's cybersecurity capabilities, and collaborate with international partners to address cybersecurity concerns.²⁰⁴ In addition, the Finnish government formed the Finnish Transport and Communications Agency (Traficom), which is in charge of guaranteeing the security of Finland's communications networks.²⁰⁵

Singapore has undertaken efforts to resolve cyberspace sovereignty challenges through its Cybersecurity Strategy.²⁰⁶ The policy includes efforts to secure key infrastructure, improve the cybersecurity capabilities of Singaporean businesses and individuals, and collaborate with international partners to address cybersecurity concerns. The Singaporean government has also formed the Cyber Security Agency (CSA), which is in charge of advising businesses and people on cybersecurity matters.²⁰⁷

Therefore, domestic legal instruments and policy frameworks are beneficial in resolving cyberspace sovereignty challenges. The UK, Germany, France, Finland, and Singapore have all enacted cybersecurity measures to defend their population and key infrastructure from cyber attacks. These domestic frameworks are critical for maintaining a safe and secure digital environment as well as dealing with the complex legal challenges that arise in cyberspace.

5. Conclusion

The rapid digital transformation of society has presented unique opportunities and challenges, particularly at the regional and domestic levels. As cyberspace becomes increasingly integral to daily life, the need for robust regional collaboration and effective domestic strategies has become more pressing. Countries and regional organisations are navigating this complex landscape with tailored legal frameworks and policies aimed at addressing the multifaceted threats posed by ICT vulnerabilities.

201 France (n 124).

202 ANSSI (n 118).

203 Ministry of Foreign Affairs of Finland (n 162).

204 *ibid.*

205 'New approaches to regulating transport in Finland: Case study on the Transport and Communications Agency (TRAFICOM)' (OECD Library) <www.oecd-ilibrary.org/sites/a3fe77bc-en/index.html?itemId=/content/component/a3fe77bc-en> accessed 11 April 2023; Traficom, 'About Traficom' (Traficom) <www.traficom.fi/en/traficom/about-traficom> accessed 11 April 2023.

206 Singapore Government Agency (n 183).

207 Singapore Government Agency (n 185).

Regional initiatives have demonstrated the value of cooperative approaches in combating cyber threats. Frameworks such as the EU's cybersecurity directives and ASEAN's regional strategies highlight the importance of harmonising efforts across member states. These initiatives not only enhance cybersecurity capabilities but also foster shared standards that allow for coordinated responses to emerging threats. The adaptability of these regional frameworks is a critical factor in ensuring their relevance in an ever-evolving digital environment.

At the domestic level, nations have implemented a diverse array of legal instruments and policies to address specific cybersecurity challenges. For instance, countries like the UK and Germany have developed comprehensive national strategies to protect critical infrastructure, while Singapore and France have emphasised data protection and privacy through forward-thinking legislation. These domestic efforts reflect the distinct priorities and resources of individual states, demonstrating the necessity of tailored approaches to cyber governance.

The intersection of regional and domestic strategies underscores the importance of collaboration in addressing cybersecurity challenges. By aligning domestic priorities with regional objectives, states can build resilient frameworks that are both locally effective and regionally cohesive. This synergy ensures that the dynamic nature of cyber threats is met with equally dynamic solutions, capable of safeguarding both national and regional interests.

In an era defined by rapid technological advancement, the future of cybersecurity governance lies in the ability of regional and domestic actors to innovate and adapt. Through continued cooperation and the refinement of legal and policy frameworks, nations and regions can establish a robust defense against the complexities of cyberspace while fostering an environment of security, trust, and shared progress.

Non-International Armed Conflicts And New Technologies: Reconceptualizing The Intensity Criterion

*Giulia Baj**

PhD in International Law

ORCID 0000-0002-6231-9805

DOI: 10.54103/milanoup.215.c446

Abstract

Technological developments affect every aspect of human life, warfare included, suffices to recall the emergence of the so-called cyber-attacks, unmanned robots, autonomous weapon systems. Consequently, new technologies affect international humanitarian law (IHL) as well. Among the various legal questions arisen by the introduction of new technologies in warfare, their impact on the criterion of intensity required for the classification of a situation as a non-international armed conflict (NIAC) is here assessed. How is the reaching of such a threshold measured, when new weapons are more and more precise? How should this criterion be evaluated, in cases in which there are not casualties – both military and civilians – at all, a situation that may happen in case of cyber-attacks? This problem is conceptually and practically relevant, as a NIAC exists only when the criterion of intensity – together with the criterion of organization – is reached, thus allowing the application of IHL. The development of the criterion of intensity is first assessed, resorting to conventional rules interpreted under the rules of the Vienna Convention on the Law of Treaties and international case law, of the International Criminal Tribunal for the Former Yugoslavia (ICTY) in particular. After this initial assessment, the work of reconceptualization of the criterion of intensity is conducted, submitting an approach based on the protection of human rights. This approach would allow a reconceptualization of the criterion of intensity, in view of the new technological weapons, which complies with the scope of the rules of IHL and is consistent with the development of international law on a more general level.

* The views expressed in this publication are solely those of the author and do not represent the positions of any institutions or organizations they have been affiliated with.

Keywords

International Humanitarian Law, Armed Non State Actors, Non International Armed Conflicts, Intensity Criterion, Organization Criterion, Cyber Warfare, Unmanned Weapons

1. Introduction

The evolution of technology affects every aspect of human life, warfare included. In recent years, we have witnessed significant evolutions in this regard, from the usage of more or less sophisticated weaponized robots to the resort to cyber-attacks. These developments have had, and are having, significant impacts on many aspects of International Humanitarian Law (IHL). Among the several emerging issues, the impact of new weapons on the intensity criterion required for the identification of non-international armed conflicts (NIACs¹), which are those armed conflict that involve at least one non state armed group (NSAG), is here assessed. Indeed, the topic is interesting for several reasons, relating both to the particular method of identification of NIACs, and to the peculiar characteristics of this type of armed conflicts. In addition, given the widespread diffusion of NSAGs and NIACs,² the topic appears particularly significant in the present international scenario.

Regarding the issue of the identification, there exists a peculiar method to assess the existence of a NIAC; in fact, the latter must be tested on two criteria, namely the level of organization of the NSAG and the level of intensity of the armed violence.³ In other words, a situation of armed violence amounts to a NIAC – thus leads to the application of IHL – only if it reaches the required minimum thresholds of organization and intensity. Given this, with specific reference to the intensity criterion, the identification of a NIAC, and the consequent application of IHL, may be severely affected by the development of technologically advanced means of warfare. The issue may become more and more relevant, as the usage of technologically advanced devices in armed conflicts will become more and more common.⁴

1 The term NIACs is here used to refer to protracted armed confrontations occurring between governmental armed forces and the forces of one or more armed groups, or between such groups arising on the territory of a State party to the Geneva Conventions, following the definition provided by the International Committee of the Red Cross (ICRC). See ICRC, 'How Is the Term "Armed Conflict" Defined in International Humanitarian Law?' (ICRC 2008).

2 See, eg, Geneva Academy of International Humanitarian Law and Human Rights, 'Today's Armed Conflicts' <<https://geneva-academy.ch/galleries/today-s-armed-conflicts>> accessed 29 March 2023.

3 The other one is the level of organization of the NSAGs.

4 For instance, the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, in its 2021 Final

Second, NIACs have at least one unique feature: they always involve at least one NSAG. This element cannot be ignored, as NSAGs present peculiar characteristics; they often do not have the monetary resources of States, nor the organization and training capabilities of the latter. Given all this, it appears that some types of new weapons and ways of conducting warfare will be more and more frequently used by NSAGs. In particular, drones and cyber-attacks may acquire a more and more relevant role in warfare for NSAGs. Indeed, the former are becoming easy to get and use, as well as cheaper and cheaper; this is particularly true in regard to repurposed, weaponized civilian drones. In addition, cyber-attacks may be conducted also by individuals located in different areas. Given that NSAGs often do not have ample resources and are frequently composed by people coming from different areas, the characteristics of drones and cyber-attacks may appear particularly appealing for NSAGs. On the other hand, the military forces of States may have access to sophisticated, technologically advanced weapons, such as drones specifically created for warfare activities. Moreover, given the ample diffusion of ICTs, they may have specific units dedicated to cyber activities. Despite being deeply different, these means of warfare share a common feature: they are all capable of producing not very intense attacks. Consequently, their usage may affect the concept of intensity, as it has been developed up until now.

These issues may have significant practical impacts. Indeed, the existence of an armed conflict (both international and non-international) leads to the application of a specific set of rules, namely the rules of IHL. This is true for armed conflicts conducted resorting to technologically advanced means of warfare as well.⁵ This is particularly relevant, as the IHL legal framework establishes peculiar rules, which may deeply differ from the rules applicable in peacetime. For instance, the regulation provided in case of detention may deeply vary, depending on whether the detention takes place in peacetime or during an armed conflict towards members of the armed forces of the enemy; in fact, in this

substantive record, affirmed that the use of ICTs, both by States and NSAGs, is becoming more likely. Open-ended working group on developments and in the field of information and telecommunications in the context of international security, 'Final Substantive Report' (10 March 2021) A/AC.290/2021/CRP.2.

5 Several position papers submitted by States affirm that international law, IHL included, applies to the cybernetic field and that no specific legal framework is needed. See, eg, Italian Ministry for Foreign Affairs and International Cooperation, 'Italian Position Paper on "International Law and Cyberspace"' (2021). Coherently, r 20 of the Tallinn Manual 2.0 states that '[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict'. Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) r 20. Even though it is not binding, the Tallinn Manual is a scholarly work of collection and explanation of the rules applicable to cyberwarfare, conducted with the involvement of States and based on the practice, official statements and activities of States, academic research, and multi-stakeholders' initiatives. Hence, despite its non-binding nature, it is a significant instrument to assess the rules applicable in this type of warfare.

second hypothesis the IHL legal framework shall apply.⁶ IHL sets specific rules for NIACs as well, thus their identification as equally relevant as the identification of international armed conflicts.

To assess the impact of new warfare technologies on the criterion of intensity, necessary for the existence of a NIAC, a brief overview of the characteristics of the new weapons is conducted. Since NSAGs are a necessary party of NIACs, this assessment focuses on drones and cyber-attacks, which may become the weapons of choice of NSAGs. Particular attention is paid to the limited intensity of the attacks conducted with new means of warfare.

Then, the concept of intensity under IHL is assessed. To do so, the most relevant international provisions are examined and interpreted also resorting to the *travaux préparatoires*, as well as the most important case law on the matter at issue. Last, several theories on the reconceptualization of the intensity criterion considering the latest developments are presented. In this sense, it appears that a return to the original aims of IHL, with a stronger consideration of the protection of human dignity and human rights, may be the best option. However, the evolution of warfare presents several other problems in the application of IHL. Consequently, the call for a wider reconceptualization of IHL taking into consideration the wider role gained by international law of human rights (IHRL) is finally made.

2. State of the art weapons, repurposed devices and current warfare in NIACs

It is a truism that the use of the latest technology in warfare is not a novelty. To mention just one example, dozens of world-renowned scientists, coming from all over the world, took part in the research on atomic energy that led to the production of the atomic bombs, used during the Second World War (WWII)⁷. Present day is no different: new technologies are used for warfare activities. However, current technological developments in the field present original aspects, which may affect the concept of intensity as required element for the existence of a NIAC. Considering technological innovations regarding both the weapons and warfare activities most often accessible to NSAGs and those available to States, it is important to highlight that, despite being deeply different, they may cause only minimal, if any, losses. Some types of unmanned

6 See, in particular, Geneva Convention III Relative to the Treatment of the Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135.

7 See, eg, Henry De Wolf Smyth, *Atomic Energy for Military Purposes: The Official Report of the Development of the Atomic Bomb under the Auspices of the United States Government, 1940-1945* (2nd edn, Stanford University Press 1989).

vehicles, as well as cyber-activities, constitute a good example of this type of weapons.

Unmanned vehicles, especially but not only aerial ones⁸ (unmanned aerial vehicles will be called drones hereinafter⁹), have been used for military purposes for decades. Today, however, we assist to a two-pronged evolution, ultimately caused by a single phenomenon: technological developments. On the one hand, State armed forces are getting equipped with technologically advanced drones;¹⁰ normally the latter are highly precise and able to kill one particular individual without any other casualty. For instance, in 2022 the Central Intelligence Agency (CIA) of the United States killed the Taliban leader Ayman al-Zawahiri using two Hellfire missiles, launched by a drone. According to the US intelligence, all the other people present in the same building were uninjured.¹¹

On the other hand, drones are also becoming a weapon of choice of NSAGs, that usually do not have the economic resources States have. Today there exist various types of drones, which are more or less sophisticated and more or less expensive; given this variety, it appears that when discussing NIACs and NSAGs the most relevant type of drone may be the hobbyist one, as it can be considered as a new type of “cheap” weapons. Hobbyist drones were created and are produced for civilian purposes, and in fact it is easy to have access to them¹² and they are easy to use. However, they can be easily repurposed and weaponized, for instance by installing remotely controlled bombs on them; moreover, as they have small dimensions, they can easily elude radar controls.¹³ Because of this disruptive potential, this type of drones has already been used for warfare activities.¹⁴ Undeniably, the drones used by NSAGs may be less effective than more technologically advanced weapons; this means that the intensity level required by international law for rules of IHL to apply may

8 See, eg, Thomas P Ehrhard, ‘Air Force UAV’s: The Secret History’ (Mitchell Institute Press, July 2010) <<https://apps.dtic.mil/sti/pdfs/ADA526045.pdf>> accessed 30 May 2024; Peter Bergen, Melissa Salyk-Virk and David Sternman, ‘World of Drones’ (*New America*, 30 July 2020) <<https://apps.dtic.mil/sti/pdfs/ADA526045.pdf>> accessed 20 February 2023.

9 Ehrhard (n 8).

10 See, eg, Kelley Sayler, ‘A World of Proliferated Drones: A Technology Primer’ (Center for a New American Security, 2015) <<https://www.cnas.org/publications/reports/a-world-of-proliferated-drones-a-technology-primer>> accessed 30 May 2024.

11 See, eg, Redazione ISPI Online Publications, ‘Uccisione Di Ayman Al Zawahiri’ (*ISPI - Istituto per gli Studi di Politica Internazionale*, 2 August 2022) <www.ispionline.it/it/pubblicazione/uccisione-di-ayman-al-zawahiri-35932> accessed 8 April 2023.

12 Given their civilian purpose, many States do not require the registration of hobbyist drones. See, eg, Sayler (n 10).

13 As already happened to the Hezbollah’s Mohajer 4, that eluded Israeli radar because of its limited size. See *ibid*.

14 With regard to NSAGs, both Hamas and Hezbollah have employed midsize, military-grade systems, variants to the Iranian Ababil-1 and Mohajer 4. See, eg, *ibid*.

not be attained – at least for the time being¹⁵. To sum up, the acts conducted by both state-of-the-art drones available to states and repurposed drones used by NSAGs may not reach the degree of intensity required for a NIAC to come into place.

Another type of new means of warfare is cyber-attacks. The latter may appeal to NSAGs as well; in fact, members of NSAGs may live in different areas, and NSAGs may not have the necessary structure to organize their activities. Also, cyber-attacks surely require particular skills, but do not require great economic resources. As NSAGs often have limited funds and their members are often scattered in different places, they may consider cyber-attacks as a preferable warfare activity. It should be noted that the resort to cyber-attacks by NSAGs is not such a recent phenomenon: in 2010, Mohamedou Ould Slahi, suspect in a terrorism case, affirmed that Al Qaeda conducted cyber-attacks, also against Israeli governmental computers, in 2001.¹⁶ Also, it can be inferred that, as time went by, NSAGs have only acquired more and more skills.¹⁷

However, cyber-attacks may not cause losses at all; after all, cyber-attacks do not have the physical component of kinetic warfare activities. However, they may severely affect their target. To provide a few examples, in recent years severe, large-scale cyber-attacks have been conducted against national informatic systems. For instance, in August 2022 the informatic systems of Estonian public and private institutions suffered an impressive cyber-attack,¹⁸ but it did not cause any casualty. 15 years before, Estonia was the victim of another, impactful cyber-attack, as in 2007 a series of cyber-attacks was conducted against the websites of several Estonian organizations and institutions, including banks, ministries, and the Parliament.¹⁹ Allegedly, these cyber-attacks followed the removal of the statue of the Bronze Soldier of Tallinn, a statue posed during the Soviet era to commemorate the Russians died while pushing the Nazis outside

15 The technological development in the field of unmanned vehicles is indeed undergoing a process of rapid evolution. See, eg, Bergen, Salyk-Virk and Sternman (n 8).

16 Christopher D DeLuca, 'The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors' (2013) 3 Pace International Law Review Online Companion 278.

17 See, in this regard, the statement of the UK Secretary of State for the Home Department: 'There will be more cyber terrorism. Groups will continue to benefit from the off-the-shelf technology in planning and conducting attacks, making operations more secure and potentially more lethal. The Internet and virtual space will be strategically vital'. Secretary of State for the Home Department, 'Contest: The United Kingdom's Strategy for Countering Terrorism' (July 2011) 41, in DeLuca (n 16) 292.

18 Pascale Davies, 'Estonia Hit by "most Extensive" Cyberattack since 2007 amid Tensions with Russia over Ukraine War' (*Euronews*, 19 August 2022) <www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain> accessed 8 April 2023.

19 James Pamment and others, 'Hybrid Threats: 2007 Cyber Attacks on Estonia' (NATO Strategic Communication Centre of Excellence 2019).

the Country at the end of WWII.²⁰ While the attribution of the responsibility for this attack, and the role of the Russian State in it, has been widely discussed, no unanimous conclusion has been reached.²¹ These cyber-attacks lasted for weeks. It has been said that '[i]t was the first time cyber attacks threatened the security of an entire nation'.²² Moreover, the damages caused by the cyber-attack provoked a series of riots, which led to property damage, several people injured and one death.²³ While these cyber-attacks caused serious denials of service, they did not directly cause any casualty, and indirectly caused only one death.

This brief excursus leads to the conclusion that several new means of warfare may not reach the degree of intensity, which is required today for a NIAC to take place. Weaponized drones often do not have the impact required to satisfy the intensity criterion, and cyber-attacks cannot cause deaths directly. Given all this, when discussing the way to identify a NIAC the impact on the threshold of intensity of these technologically advanced weapons must be discussed.²⁴

3. Intensity criterion for the existence in NIACs in IHL and international case law

While the concept of international armed conflicts (IACs) is based on a clear, conventional provision,²⁵ NIACs do not have a similarly clear definition. Nonetheless, they have been regulated by different provisions of IHL, most notably by the common article 3 to the Four Geneva Conventions on the Law of

²⁰ See, eg, DeLuca (n 16).

²¹ *ibid.*

²² Scott J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 *Berkley Journal of International Law* 192, in DeLuca (n 16) 286.

²³ Shackelford (n 22) 193, in DeLuca (n 16) 286.

²⁴ Given the topic at issue, the analysis considers conducts attributable to NSAGs, and thus not attributable to States.

²⁵ Under common article 2, an IAC is 'a declared war or [...] any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them'. Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31; Geneva Convention II for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85; Geneva Convention III Relative to the Treatment of the Prisoners of War (n 6); Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War' (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 common art. 2. However, it should be noted that the identification of IACs may be affected by the emergence of new technologies as well. For instance, at the moment it is not unanimously accepted under what circumstances cyber-operations fall into the scope of usage of armed force. This affects the application of the rules of IHL, as well as art. 2(4) of the UN Charter.

War (CA3) and by the Additional Protocol II to the Four Geneva Conventions on the Law of War (APII). Thus, the relevant provisions on the material field of application of CA3 and APII, which are contained in CA3 itself and art 1(2) APII shall be taken as a starting point for the assessment of the intensity criterion. The matter has then been further clarified by international courts, especially by the International Criminal Tribunal for the former Yugoslavia (ICTY) in its case law. All this led to the development of a dual test for the existence of a NIAC, based on the presence of a minimum level of organization and intensity.

The concept of NIAC itself and the scope of the criteria have been developed over time. Consequently, it appears useful to start the analysis from the interpretation of conventional provisions on NIACs, with the support provided by authoritative doctrine; in this sense, reference to the International Committee of the Red Cross (ICRC) Commentaries in particular is made. Then, the analysis moves to the most relevant international case law. Last, the most significant issues relating to the concept of intensity, and the approaches submitted to solve them, are presented. This analysis, however, leads to the conclusion that this concept does not have a strictly determined scope.

The examination of the conventional law dedicated to NIACs and the concept of intensity regards two provision in particular, CA3 and art 1 APII. Even though CA3 established the minimum set of rules applicable in case of conflicts not of an international character,²⁶ it does not provide a definition of this type of conflicts. In fact, it only establishes its application in case of 'armed conflict not of an international character occurring in the territory of one of the High Contracting Parties'.²⁷ This provision thus appears quite tautological, as it establishes that, for it to apply and regulate NIACs, it is necessary for a NIAC to occur. It does not provide any other indication of what a NIAC is. However, the interpretation of this article, taking into consideration also its *travaux préparatoires*, leads to the conclusion that a minimum level of intensity was considered as a necessary requirement to identify a NIAC, and ultimately to apply the other provisions of CA3. In order to correctly frame CA3, first, the motivation and the consequences of such a limited definition are briefly provided, then its established interpretation is presented.

It has been affirmed that this laconic provision has to be connected to the reluctance of States, that participated in the Diplomatic Conference which led to the adoption of the Geneva Conventions, to regulate with rules of international

26 Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (n 25); Geneva Convention II for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (n 25); Geneva Convention III Relative to the Treatment of the Prisoners of War (n 6); Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War (n 25) common art. 3.

27 *ibid.*

law (as rules of IHL) non-international armed conflicts have always been perceived as falling within the domestic realm.²⁸ Indeed, CA3 was the first international provision to deal with non-international conflicts. It should be noted that this laconic provision ran the risk of producing unexpected, unwanted consequences. In fact, it was stated that such a ‘vague’²⁹ provision constituted a threat to States that feared ‘it might be taken to cover any act committed by force of arms – any form of anarchy, rebellion, or even plain banditry’,³⁰ ultimately compressing their sovereignty on domestic issues. Undeniably, the text of CA3 does not offer a clear definition of what a NIAC is.

Nonetheless, it is possible to reconstruct the relevance of the intensity criterion even from this laconic provision. This can be done applying the criteria for treaty interpretation set in the Vienna Convention on the Law of Treaties, in particular resorting to a systematic interpretation, and thus reading the provision in the context of the whole convention,³¹ and to the *travaux préparatoires*, as a supplementary means of interpretation in case of an obscure interpretation of a provision.³²

Under the systematic interpretation, CA3 should be first of all interpreted taking into consideration common article 2 to the Four Geneva Conventions (CA2). The latter sets the application of the Geneva Conventions ‘to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties’, thus IACs.³³ Therefore, CA3 may be

28 See, eg, ICRC, Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Commentary of 2016’ (2016) para 416 <<https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/toc/commentary/2016>> accessed 17 April 2023. See also Schmitt (n 5) r 23 para 16.

29 See, eg, Jean S Pictet, *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (ICRC 1952) 49.

30 See, eg, *ibid.*

31 Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331 art 31(1), 31(2). ‘A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose. The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes: (a) any agreement relating to the treaty which was made between all the parties in connection with the conclusion of the treaty; (b) any instrument which was made by one or more parties in connection with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty’.

32 *ibid* art 32. ‘Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31: (a) leaves the meaning ambiguous or obscure; or (b) leads to a result which is manifestly absurd or unreasonable’.

33 Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (n 25); Geneva Convention II for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (n 25); Geneva Convention III Relative to the Treatment of the Prisoners of War (n 6); Geneva

interpreted *a contrario* as applicable in cases of armed conflicts that did not arise between two or more High Contracting Parties, but rather a High Contracting Party and one or more NSAGs, or two or more NSAGs against each other in the territory of one High Contracting Party. This interpretation appreciates the differences between the two articles, that address both the same issue, namely the scope of material application of the rules of IHL established in the Geneva Conventions.³⁴

Assessing the *travaux préparatoires*, it should be noted that already the 1952 Commentary by the ICRC referred to the discussion that led to the final draft of CA3 and this discussion has been recalled ever since in the following ICRC Commentaries on the Four Geneva Conventions.³⁵ Thus, it appears that, in its commentaries, the ICRC has been resorting to these preparatory documents for decades. In particular, the 1952 ICRC Commentary included a list of ‘convenient criteria’,³⁶ which were discussed as a list of amendments while drafting CA3 as not obligatory but useful to identify a NIAC. In particular, these criteria may help distinguishing NIACs ‘from a mere act of banditry or an unorganized and short-lived insurrection’.³⁷ From the latter expression it emerges that the ICRC believes that a minimum degree of intensity is necessary for a NIAC to take place. This is consistent with the content of these ‘convenient criteria’, as they include, among others, that NSAGs should have the ability to engage in conflicts with the State authorities,³⁸ and that NIACs should include the cases in which ‘the legal Government is obliged to have recourse to the regular military forces against insurgents’.³⁹ It can thus be inferred that, according to these criteria, NIACs differ from acts of banditry and short-lived insurrections as the former must present a higher degree of intensity. Despite its brevity, the interpretation of CA3 under a systematic criterion and considering the *travaux préparatoires* leads to the conclusion that this article implicitly requires a necessary minimum level of intensity for a NIAC to take place.

Convention IV Relative to the Protection of Civilian Persons in Time of War (n 25) common art 2.

34 International Committee of the Red Cross, Convention (III) Relative to the Treatment of Prisoners of War. Commentary of 2020 paras 427ff (*International Committee of the Red Cross*, 2020) <<https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=E362C510EB54A83FC12585B500590D0F>> accessed 16 September 2022.

35 See, eg, International Committee of the Red Cross, ‘Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Commentary of 2016’ (n 28) para. 419.

36 Pictet (n 29) 49.

37 *ibid* 50. Cited in following Commentaries, eg, International Committee of the Red Cross, Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Commentary of 2016’ (n 28).

38 Pictet (n 29).

39 *ibid* 49–50.

Last, the presence of a minimum requirement of intensity appears coherent with the already mentioned reluctance showed by States during the process of adoption of CA3. In this regard, the demand of a minimum level of intensity appears as the way to dispel such fears. Indeed, ‘Common Article 3’s radical nature necessitated strict constraints – including the intensity threshold – to alleviate state concerns [...] States’ reluctance to recognize the existence of a NIAC necessitated a clear means of distinguishing NIACs from internal disturbances of lesser severity. Accordingly, from its inception, Common Article 3 was understood to apply only once an internal conflict reached a certain level of intensity’.⁴⁰ In conclusion, despite the limited text, it appears that CA3 already set the necessity of a minimum level of organization as a necessary element for the existence of a NIAC, and the consequent application of the rules of IHL.

The matter of the criterion of intensity was more explicitly addressed in APII. This Protocol regards the protection of victims of NIACs, consequently its field of application strictly depends on the definition of NIACs. Accordingly, its art 1, titled ‘Material field of application’, clarifies the circumstances in which APII shall apply. Before its assessment, it should be noted that this article affirms that it ‘develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application’; thus, even though this article differs, in some parts, from CA3,⁴¹ it is an expansion of the provision set therein. Relevant for the matter at issue, art 1(1) APII states it shall apply to those armed conflicts ‘which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol’.⁴² Moreover, in its final part art 1 APII affirms that it ‘shall not apply to situations of internal disturbances and tensions, such as riots, isolated and

40 Oona A Hathaway and others, ‘Consent Is Not Enough: Why States Must Respect the Intensity Threshold in Transnational Conflict’ (2016) 165 *University of Pennsylvania Law Review* 1, 12.

41 In particular, APII shall apply ‘to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol’. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 (Additional Protocol II) art 1. Therefore, APII introduces a new requirement: the armed conflict must occur between one or more NSAGs and the armed forces of a State.

42 *ibid* art 1(1).

sporadic acts of violence and other acts of a similar nature, as not being armed conflicts'.⁴³ Later, this provision has been included in the Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict.⁴⁴ Thus, the intensity requirement is established both by reference to the characteristics of the relevant military operations, and in a negative manner, as art 1 APII explicitly establishes what cannot be considered a NIAC because of its not intense enough nature.

While the two main conventional provisions of IHL on the topic at issue do not present the same definition of NIAC, some common conclusions on the intensity required for the existence of a NIAC can be drawn. In particular, both require the reaching of a minimum level of intensity, in order to distinguish a NIAC from internal riots or disturbances, or other acts which do not fall into the scope of NIACs. Therefore, and with particular reference to CA3, it can be inferred that the degree of intensity has been a requirement for the existence of a NIAC since the first post-WWII regulations on the matter. Such a requirement has been confirmed and clarified in subsequent international case law, as will be shown in the following paragraph.

Over time, the concept of NIAC has been assessed by international case law as well. In this regard, the jurisprudence of the ICTY should be recalled, its *Tadić* case in particular. In it, the ICTY had to identify what a NIAC is, in order to evaluate whether or not an armed conflict was taking place when the alleged offences object of the case were committed. In this regard, it affirmed that 'an armed conflict exists whenever there is a resort to armed force between States or *protracted armed violence between governmental authorities and organized armed groups or between such groups within a State*' (emphasis added).⁴⁵ This definition has been confirmed not only by the ICTY in subsequent cases, but also by other international courts, such as the International Criminal Tribunal for Rwanda,⁴⁶ and the International Criminal Court.⁴⁷ Regarding the latter, it should be also recalled that the Statute of the International Criminal Court adopted the *Tadić* approach in the formulation of NIACs in art 8(2)(f).⁴⁸

43 *ibid* art 1(2).

44 'This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature'. Second Protocol to The Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict (adopted 26 March 1999, entered into force 9 March 2004) 2253 UNTS 172 art 22 (2).

45 *The Prosecutor v Dusko Tadić (Appeals Chamber, Decision on The Defence Motion for Interlocutory Appeal on Jurisdiction)* [1995] International Criminal Tribunal for the former Yugoslavia IT-94-1-I para. 70.

46 *Prosecutor v Akayesu* (Judgement) ICTR-96-4-T, T Ch I (2 September 1998).

47 See, eg, *Prosecutor v Lubanga Dyilo* (Judgement) ICC-01/04-01/06 (14 March 2012); *Prosecutor v Al Mabdi* (Judgement and Sentence) ICC-01/12-01/15 (27 September 2016).

48 'Paragraph 2 (e) [applying to NIACs] applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as

The evolution of the concept of NIACs here briefly presented led to the definition provided in 2008 by the ICRC: ‘Non-international armed conflicts are *protracted armed confrontations* occurring between governmental armed forces and the forces of one or more armed groups, or between such groups arising on the territory of a State [party to the Geneva Conventions]. The armed confrontation must reach a *minimum level of intensity* and the parties involved in the conflict must show a *minimum of organisation*’⁴⁹ (emphasis in the original text). This definition has been widely accepted. For instance, Rule 23 of the Tallinn Manual states that ‘[a] non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organization’⁵⁰.

In conclusion, the test of the existence of a NIAC continues to rest on the reaching of a minimum threshold of two requirements, one of them being the criterion of intensity. However, the rapid evolution of warfare due to the more and more frequent usage of technologically advanced weapons, both by States and NSAGs, may be deeply affect this criterion. To tackle this issue, the concept of intensity should be assessed first.

4. Defining the scope of the concept of intensity

Taking into consideration both the conventional and case law, as well as the definition provided by the ICRC in 2008, a series of conclusions can be drawn. First, the involvement of State armed forces is not considered as necessary for the existence of a NIAC; this consistent with CA3 but contrary to art 1 APII. It may thus be inferred that APII has a more limited material field of application, consequently the legal framework of APII may apply to a limited series of circumstances, the ones able to reach the higher threshold set in its art 1. Second, the two criteria of intensity and organization are required for a NIAC to take place. However, the presence of two criteria requires the balance between the two. Third, and the element of novelty, the armed violence must be ‘protracted’. This latter element was introduced by the ICTY and led to many debates

riots, isolated and sporadic acts of violence or other acts of a similar nature. It applies to armed conflicts that take place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups’. Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 (ICC Statute) art 8(2)(f).

49 ICRC, ‘How Is the Term “Armed Conflict” Defined in International Humanitarian Law?’ (n 1) 5.

50 Schmitt (n 5) r 23.

on its scope. Last, the *Tadić* case itself, as well as subsequent ICTY judgements, mentioned a series of factors to take into consideration when assessing whether a certain situation amounted to a NIAC or not. Nonetheless, the exact scope of these factors has been object of discussion. These issues are now discussed, before attempting at the reconceptualization of the criterion of intensity in the light of new technological developments applied to warfare.

Since the relationship between the adjective ‘protracted’ and the concept of intensity is one of the debated issues, it appears useful to assess whether the two are related – in other words, whether the intensity has to be protracted to reach the level required for the existence of a NIAC. First of all, it has to be noted that from a lexical point of view, the adjective ‘protracted’ cannot be considered as a synonym of ‘intense’, as the former has a time-focused connotation the latter does not possess.⁵¹ Therefore, it refers to the duration of the armed violence, rather than to its intensity. It should be highlighted that the element of duration does not correspond even to the concept of continuity. As noted by the Commentary to Rule 23 of the Tallinn Manual, the armed violence to reach the required degree of intensity ‘need not to be continuous in nature’.⁵² Consistent with this semantic approach, it has been affirmed that the expression ‘protracted armed violence’ may infer that duration should be considered as part of the evaluation of the requirement of intensity; however, as already said it is only *part* of this evaluation, thus the two concepts are not the same. On the contrary, it is feasible to imagine situations of armed violence in which the intensity threshold is reached, even without the requirement of the duration. In this sense, the ICRC affirmed that ‘[t]he duration of hostilities is thus appropriately considered to be an element of the assessment of the intensity of the armed confrontations. Depending on the circumstances, hostilities of only a brief duration may still reach the intensity level of a non-international armed conflict if, in a particular case, there are other indicators of hostilities of a sufficient intensity to require and justify such an assessment’.⁵³ The thesis submitting that the duration of the armed violence is only one part of the concept

51 “Protracted: lasted for a long time or made to last longer than necessary”. Merriam-Webster, ‘Protracted’ (2022); “Intense: existing in an extreme degree”. Merriam-Webster, ‘Intense’ (2023).

52 Schmitt (n 5) r 23 para 9.

53 ICRC, ‘Convention II for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Commentary of 2017’ (2017) para 462 <<https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949>> accessed 17 April 2023. The Commentary makes reference to the *Tablada* case, in which the Inter-American Commission on Human Rights, generally applying the criteria of intensity and organization, came to the conclusion that an attack by 42 armed persons against an army barracks, leading to combat lasting about 30 hours, had crossed the threshold of a non-international armed conflict’. *ibid* note 148. Citing *Abella v Argentina (Tablada)* Inter-American Commission on Human Rights 11.137, OEA//Ser/L/V/II.98 (18 November 1997).

of intensity is supported by case law as well. In this regard, other ICTY cases that clarify that the concept of intensity cannot only be based on the duration requirement should be recalled. As reported in the *Boškoski & Tarčulovski* case, '[v]arious indicative factors have been taken into account by Trial Chambers to assess the 'intensity' of the conflict'.⁵⁴

Consequently, it has been submitted that '[t]he thumbnail version is that on its face the key textual formulation requires armed violence to be sufficiently long, but in jurisprudence that duration dimension is often incorporated into a broader analysis of the intensity of hostilities as but one criterion concerning the existence (or not) of a non-international armed conflict'.⁵⁵ It can thus be deduced that international case law has developed the concept of the requirement of intensity, which has to be 'protracted' in order to distinguish common riots and disturbances from armed conflicts, while at the same time not requiring a long duration of the hostilities. This position is also supported in the Tallinn Manual, as the commentary to Rule 23, 'Characterization as non-international armed conflict', states that '[s]poradic cyber incidents, including those that directly cause physical damage or injury, do not [...] constitute non-international armed conflict'.⁵⁶ After all, a rigid requirement of duration would impair one of the goals of IHL. If the application of the guarantees of IHL and the possible intervention of international organization such as the Red Cross depends on the existence of a protracted armed violence, interpreted on a time-focused criterion, then there would be a period of uncertainty regarding the application of the rules of IHL, especially at the beginning of the hostilities.⁵⁷ However, it should be noted that, despite the ample recognition in international case law, the sharp distinction between intensity and duration has not gained unanimous support.⁵⁸

The flexibility in the process of evaluation appears also in the relationship between the two criteria of intensity and organization, with particular reference to the balance of the two. In this regard, discussing the topic at issue in its 2020 Commentary to the Geneva Convention (III), the ICRC affirmed that 'the criteria of intensity and organization must be present *cumulatively* in order

54 *Prosecutor v Boškoski and Tarčulovski* (Trial Judgement) IT-04-82-T (10 July 2009) para 177.

55 Dustin A Lewis, 'The Notion of "Protracted Armed Conflict" in the Rome Statute and the Termination of Armed Conflicts under International Law: An Analysis of Select Issues' (2019) 101 *International Review of the Red Cross* 1091, 1099.

56 Schmitt (n 5) r 23 para 5.

57 See Marco Sassòli and Julia Grignon, 'Les Limites Du Droit International Pénal et de La Justice Pénale Dans La Mise En Oeuvre Du Droit International Humanitaire' [2012] *Le droit international humanitaire face aux défis du XXIe siècle* 133.

58 See, eg, German Ministry of Justice, 'Code of Crimes against International Law (CCAIL)' 26 June 2002, cited in ICRC, *Convention II for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, Commentary of 2017 (n 53) note 148.

for a situation of violence to reach the threshold of a non-international armed conflict' (emphasis added).⁵⁹ Since the adjective 'cumulative' means 'made up of accumulated parts',⁶⁰ without any reference to the percentage of the components, it may be inferred that the threshold necessary for a NIAC may be reached when the two criteria combined are reached. It is not required for the two criteria to reach the same degree. This conclusion is supported by the ICRC, which even affirmed that '[d]epending on the circumstances, however, it may be possible to draw some conclusions from one criterion for the other. For example, the existence of highly intense armed confrontations between State authorities and non-State armed groups, or between several non-State armed groups, may indicate that these groups have reached the level of organization required of a Party to a non-international armed conflict'.⁶¹ Consequently, the degree of intensity may depend also on the level of organization reached by the NSAGs. This relationship between the criteria is an application of the flexible approach used to evaluate the two, ultimately to assess the existence of a NIAC.

Last, the practice of international courts to provide a list of factors to evaluate whether a situation of armed violence amounts to a NIAC or not further complicates the issue of the identification of the intensity requirement. Indeed, in the already mentioned *Boškoski & Tarčulovski* case the ICTY Trial Chamber affirmed that the factors to take into consideration to evaluate the intensity 'include the seriousness of attacks and whether there has been an increase in armed clashes, the spread of clashes over territory and over a period of time, any increase in the number of government forces and mobilisation and the distribution of weapons among both parties to the conflict, as well as whether the conflict has attracted the attention of the United Nations Security Council, and whether any resolutions on the matter have been passed. Trial Chambers have also taken into account in this respect the number of civilians forced to flee from the combat zones; the type of weapons used, in particular the use of heavy weapons, and other military equipment, such as tanks and other heavy vehicles; the blocking or besieging of towns and the heavy shelling of these towns; the extent of destruction and the number of casualties caused by shelling or fighting; the quantity of troops and units deployed; existence and change of front lines between the parties; the occupation of territory, and towns and villages; the deployment of government forces to the crisis area; the closure of roads; cease fire orders and agreements, and the attempt of representatives

59 ICRC, Convention III Relative to the Treatment of Prisoners of War. Commentary of 2020' (n 34) para 468.

60 Merriam-Webster 'Cumulative' (2023).

61 ICRC, Convention III Relative to the Treatment of Prisoners of War. Commentary of 2020' (n 34) para 468. See also Jann K Kleffner, 'The Legal Fog of an Illusion: Three Reflections on "Organization" and "Intensity" as Criteria for the Temporal Scope of the Law of Non-International Armed Conflict' (2019) 95 International Law Studies 161, 169.

from international organizations to broker and enforce cease fire agreements. At a more systemic level, an indicative factor of internal armed conflict is how organs of the State, such as the police and military, use force against armed groups'.⁶²

This flexible approach has been reaffirmed by the ICTY also in other cases. Indeed, it has been noted that '[s]uch an assertion reflects an acute awareness by the various tribunals that have addressed the issue that the application of an abstract definition of the factual situation of a NIAC, which centers on the two cumulative requirements of organization and intensity and their further refinement through a list of factors, is – far from surprisingly – a context-specific exercise'⁶³. Significantly, in the judgement of the *Haradinaj* case the Trial Chamber of the ICTY explicitly stated that 'Trial Chambers have relied on *indicative* factors relevant for assessing the "intensity" criterion, none of which are, in themselves, essential to establish that the criterion is satisfied' (emphasis added).⁶⁴ This approach can be tracked down in the case law of the International Criminal Court as well.⁶⁵ Despite its wide recognition, this flexible approach to the evaluation of the criteria of intensity and organization has not gained unanimous support. In this regard, the position of Jann Kleffner should be recalled; indeed, the author does not believe that all the factors should be considered as merely indicative,⁶⁶ and argues that some factors should be considered as determinative, 'whose absence ipso facto defeats the existence of a NIAC'.⁶⁷ Regarding intensity, the approach submitted by Kleffner is compatible with the characteristics of intensity as defined by relevant rules of IHL; in fact, it is suggested that 'one can distill the essence that the armed violence leads to the loss of life, injury, and destruction, or damage of objects, while taking the form of "fighting" – understood as armed confrontations of a military nature – between opposing parties. While this is not to suggest that one-sided armed violence – for instance, the killing of civilians or destruction of civilian objects – cannot also feature in the intensity analysis for determining the existence of a NIAC, fighting between the parties is a quintessential precondition, and as such, a determinative factor'.⁶⁸ It can thus be inferred that, even though differing doctrinal positions exist, the prevailing thesis on the evaluation of the criterion of intensity, supported by significant international case law, relies on flexibility and on a case-by-case approach.

62 *Prosecutor v Boškoski and Tarčulovski* (n 54) paras 177–178.

63 Kleffner (n 61) 168.

64 *Prosecutor v Haradinaj et al.* (Trial Judgement) IT-04-84-T (3 April 2008) para 49. See also para 60.

65 See, eg, *Prosecutor v Lubanga Dyilo* (n 47) esp. para 538.

66 'It appears doubtful, however, that *all* factors produced in the jurisprudence by the ad hoc tribunals are no more than indicative'. Kleffner (n 61) 168.

67 *ibid.*

68 *ibid* 169.

This brief analysis of the emergence, characteristics, and methods of evaluation of the intensity criterion leads to the conclusion that the latter does not have a precisely defined scope. On the contrary, the exact scope of this criterion is still unclear, and its assessment is based on a case-by-case analysis. However, it appears that this element of unclarity may be an advantage: in fact, it guarantees a flexible approach. Such an approach should be sought-after when applying the criterion of intensity to situations of warfare conducted employing new, technologically advanced weapons. In fact, it allows the identification of NIACs to evolve and adapt, following the developments of warfare. Given all this, it is now possible to reassess the concept of intensity, to accommodate the features of modern warfare.

5. Reconceptualizing the threshold of intensity in the light of new means of warfare

The emergence of new weapons can, in many cases, affect the criterion of intensity, whose perimeter has been left – arguably on purpose – unprecise. Given the growing diffusion of new weapons, it appears that it is time to reconceptualize the concept of intensity, to allow the application of the rules of IHL even in cases in which new technological weapons are employed.

First, it has to be analyzed whether there exists a limitation in means of warfare able to reach the threshold of intensity required for a NIAC to come into existence. The answer is negative; indeed, there is not any limitation to the means of warfare employed for IHL to apply. As argued in the Tallinn Manual 2.0, '[a]pplication of the law of armed conflict does not depend on the type of military operation or on the specific means and methods of warfare employed'.⁶⁹ Coherently, 'cyber operations alone, in the absence of kinetic operations, can bring a non-international armed conflict into existence'.⁷⁰

It is true that international case law has suggested that the type of weapons used may be taken into consideration when assessing whether the criterion of intensity has been satisfied. In this regard, in its *Boškoski & Tarčulovski* case the ICTY affirmed that '[t]rial Chambers have also taken into account [...] *the type of weapons used, in particular the use of heavy weapons, and other military equipment, such as tanks and other heavy vehicles*' (emphasis added).⁷¹ In other words, the ICTY stated that the type of weapons used, with particular reference to heavy weapons and military equipment, should be taken into consideration to assess whether the intensity criterion had been reached or not. Intuitively, one would conclude that armed violence conducted with the usage of light weapons could not reach the

⁶⁹ See, in this regard, Schmitt (n 5) r 23 para 2.

⁷⁰ *ibid* rule 23 para 2.

⁷¹ *Prosecutor v Boškoski and Tarčulovski* (Trial Judgement) (n 54) para 177.

required level of intensity for a NIAC to come into existence. However, this statement should be rejected for at least two reasons, ultimately coming to the conclusion that this cannot constitute an obstacle in the reconceptualization of the intensity criterion in the light of the development of new weapons. First, as already noted the ICTY itself affirmed that the factors submitted for the identification of a NIAC are indicative. Even considering the approach suggested by Kleffner, who argues for the existence of mandatory and indicative factors, the type of weapons employed does not appear to be a necessary element for the assessment of the degree of intensity. Second, although relevant, case law is always case law, addressed to specific cases, occurring in particular circumstances; as facts change, case law may become outdated. In this sense, the presence of heavy weapons and military equipment may be not considered as a relevant element for the assessment of the degree of intensity anymore. This is particularly true, taking into consideration the evolution of warfare, which is less and less relying on conventional heavy weapons and more and more prone to resort to remotely controlled light weapons.⁷² In conclusion, the type of means of warfare employed do not constitute an obstacle to reach the required degree of intensity.

Having clarified that it is possible to satisfy the intensity criterion employing any sort of means of warfare, another issue raised by these new means of warfare should be assessed. Given the relatively low impact these means produce, observers may ask themselves whether the minimum level of intensity required for the existence of a NIAC has been reached or not. In this regard, it has been affirmed that '[i]n view of the intensity threshold, cyber operations alone can trigger a non-international armed conflict in only rare cases'⁷³. Similar conclusion can be made when considering the usage of sophisticated drones. In this regard, it must be noted that the possibility to conduct this reconceptualization has already been suggested in recent years, taking into consideration the general

72 The definition of 'light weapon' can be found in the 'International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons', adopted by the UN General Assembly on 8 December 2005. In it, it is said that '[f]or the purpose of this instrument, "small arms and light weapons" will mean any man-portable lethal weapon that expels or launches, is designed to expel or launch, or may be readily converted to expel or launch a shot, bullet or projectile by the action of an explosive, excluding antique small arms and light weapons or their replicas. [...] (b) "Light weapons" are, broadly speaking, weapons designed for use by two or three persons serving as a crew, although some may be carried and used by a single person. They include, inter alia, heavy machine guns, hand-held under-barrel and mounted grenade launchers, portable anti-aircraft guns, portable anti-tank guns, recoilless rifles, portable launchers of anti-tank missile and rocket systems, portable launchers of anti-aircraft missile systems, and mortars of a calibre of less than 100 millimetres'. UNGA, 'Report of the Open-ended Working Group to Negotiate an International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons' (2005) A/60/88, Annex para 4.

73 Schmitt (n 5) r 23 para 7.

development of warfare. Among the several theories submitted, two are here presented, chosen because of their strong differences, which may ultimately lead to dramatically diverse results; the first theory is based on quantitative elements, whereas the second one is based on the behavior of State forces involved.

The first, quantitative-based theory, relies on the number of battle-related casualties to identify the threshold to be reached for a NIAC to come into existence.⁷⁴ Applying this theory to assess situations of armed violence characterized by the usage of new means of warfare (eg, drones or cyber-attacks), one has to conclude that often the minimum threshold of intensity required for a NIAC to exist is not reached. In fact, normally these means of warfare do not cause a high number of casualties. Thus, on the basis of this theory the number of battle-related casualties provoked by drones and cyber-attacks may not be sufficient to reach the minimum degree of intensity. However, several reasons lead to the conclusion that this theory should be rejected. First, it has to be noted that it has not gained wide support. Second, this approach may be too rigid; this indeed can be considered a shortcoming, taking into consideration that, as already noted, it is widely accepted that the intensity criterion has to be assessed with flexibility. The other two shortcomings of this approach regard its practical application. In fact, the exact number of casualties in contexts of armed violence may be difficult to assess, and not all the casualties due to an armed conflict are battle related.⁷⁵ Moreover, the quantitative approach may lead to the late recognition of the existence of a NIAC, thus compromising the effectiveness of the guarantees offered by the rules of IHL. Not only, if the armed conflict is characterized by a low number of battle-related casualties, such a rigid quantitative approach may lead to the conclusion that the threshold of intensity is never reached, and consequently that the rules of IHL can never be applied. This last issue is particularly relevant, as the technologically advanced means of warfare often do not produce a high number of casualties. In conclusion, the theory which conceptualizes the intensity criterion based on a quantitative approach linked to the battle-related deaths presents practical and theoretical shortcomings.

The second theory takes into consideration the behavior of States involved in the armed violence; when the state authorities have to resort to military force to combat armed violence, using methods which are incompatible with the right to life, the threshold of intensity is reached, thus a NIAC has come

74 For instance, the *Yearbook* of the Stockholm International Peace Research Institute stated that the number of 1,000 battle-related deaths is the threshold necessary for IHL to apply. The Uppsala Department of Peace and Conflict Research set the threshold at 25 battle-related deaths. See Anthony Cullen, 'Key Developments Affecting the Scope of Internal Armed Conflict in International Humanitarian Law' (2005) 183 *Military Law Review* 66.

75 *ibid* 87.

into existence.⁷⁶ Doing so, the governmental forces apply the military doctrine instead of the police doctrine; thus, the conducts must be assessed under the rules of IHL, which is applied as *lex specialis*.⁷⁷ At first glance, this theory does not present any issue in its application with situations of armed violence where technological means of warfare are employed. Indeed, this theory has several positive aspects. First, compared to the theory based on a quantitative approach, it is consistent with international practice. In fact, in addition to international doctrine,⁷⁸ in the *Boškoski & Tarčulovski* case the ICTY mentioned ‘any increase in the number of government forces’ as one of the various factors to be taken into consideration to assess the intensity criterion. Even though this factor should probably be considered as indicative, it surely implies the support of the ICTY for the evaluation of the State behavior. Second, its application limits the possibility for States to deny the existence of an armed conflict, while they are actively taking part in it. Consequently, applying this theory it is not possible for a State to be actively involved in an armed conflict, while publicly denying its existence. This would solve the long-standing issue of the recognition of an armed conflict: in fact, the resort by State to the use of the military doctrine makes the rules of IHL automatically applicable. In addition, this theory is sufficiently flexible, thus it is consistent with international law and case law.⁷⁹ Last, and unlike the theory based on a quantitative approach, it is compatible with the characteristics of warfare conducted with new weapons. In fact, the intensity threshold is reached when the governmental authorities apply the military doctrine to combat the armed violence, notwithstanding the type of warfare conducted. However, this theory suffers a practical problem difficult to overcome: it is based on the behavior of States. Given the rules that establish the applicability of IHL, this limitation does not constitute a problem for the application of the rules of APII, as the latter only applies in cases of armed conflicts taking place between the armed forces of the state and the NSAG ones.⁸⁰ However, NIACs, on the base of CA3, can occur also between NSAGs only, without any involvement of the state and its armed forces. Indeed, a NIAC can occur in cases in which ‘several factions [confront] each other without the involvement of the government’s armed forces’⁸¹. In addition, looking at current in-

76 Arne Willy Dahl and Magnus Sandbu, ‘The Threshold of Armed Conflict’ (2006) 45 Military Law and Law of War Review 369.

77 See *ibid* esp. 376–377.

78 See, eg, *ibid*.

79 See, eg, the already mentioned *Prosecutor v Boškoski and Tarčulovski* (n 54).

80 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (n 41) art 1.

81 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987) para 4461, cited in ICRC, ‘How Is the Term “Armed Conflict” Defined in International Humanitarian Law?’ (n 1) 4.

ternational reality, there exist states without any effective control over certain areas of their territory and without the ability to resort to the use of military force.⁸² Therefore, even though it has gained wide support and presents positive elements, namely its flexible nature, independence from the formal recognition of armed conflicts by states and compatibility with new, technologically advanced means of warfare, this theory is too limited in its application, and does not cover all the possible hypotheses of NIACs.

In conclusion, the theories based on a quantitative approach and on the behavior of States do not offer a solution to the issue related to the reconceptualization of the criterion of intensity required for the identification of a NIAC. However, the shortcomings of each approach may be useful to assess the elements that a reconceptualization of the criterion of intensity should have. Considering the first theory, the approach should not be rigid, and based on abstract measurements; considering the second, the approach should apply also in case of NIACs not involving governmental forces. This conclusion, as well as the unprecise scope of the criterion itself, should be kept in mind continuing the reassessment of the intensity criterion considering the development of drones and cyber activities as new means warfare.

6. Intensity: flexible approach and human rights

To conduct the operation of reconceptualization of the intensity criterion reconcilable with the new means of warfare, it appears useful to return to the origin of IHL itself. It seems indeed a logical necessity to identify the original and fundamental aims of IHL and then to reconstruct the intensity criterion in the light of the latest developments in warfare. Before starting the reconstruction of the aims and purposes of IHL, a statement of the ICRC Commentaries to the Four Geneva Conventions should be recalled: CA3 ‘should be applied as widely as possible’.⁸³ Therefore, it can be inferred that the concept of NIACs should be interpreted in an extensive manner.⁸⁴

82 The traditional example is provided by Somalia, see, eg, Ken Menkhaus, ‘Governance without Government in Somalia: Spoilers, State Building, and the Politics of Coping’ (2007) 31 *International Security* 74; Nicole Stremlau, ‘Governance Without Government in the Somali Territories’ (*Columbia Journal of International Affairs*, 9 January 2019) <<https://jia.sipa.columbia.edu/>> accessed 16 September 2022; Michael Schoiswohl, *Status and (Human Rights) Obligations of Non-Recognized De Facto Regimes in International Law: The Case of ‘Somaliland’ - The Resurrection of Somaliland Against All International ‘Odds’: State Collapse, Secession, Non-Recognition and Human Rights* (Brill Nijhoff 2004). But see, also, UN Peace and Security, ‘Former “Failed State” Somalia on Fragile Path to Progress: A UN Resident Coordinator Blog’ (*UN News*, 2021) <<https://news.un.org/en/story/2021/12/1108302>> accessed 16 September 2022.

83 Pictet (n 29) 50.

84 U.K. Ministry of Defence, ‘The Joint Service Manual of the Law of Armed Conflict’ (2004). Cited in DeLuca (n 16) 302.

Looking at the IHL legal framework as a whole, it appears that its general aim is the protection of individuals taking part in the hostilities or living in places where hostilities take place; it seeks to limit the effects of armed conflicts⁸⁵ and it is based on the concept that victims of armed conflicts must be protected.⁸⁶ This protection is usually framed in terms of injury, death, or property damage or destruction.⁸⁷ For instance, the ICRC affirmed that the Four Geneva Conventions and their Additional Protocols “contain the essential rules of humanitarian law protecting civilians, persons who are *hors de combat* and medical and religious personnel, as well as a range of protected objects such as civilian objects and medical units and transports”.⁸⁸ Going even further back in time, the three fundamental principles of IHL, namely the principle of distinction, the prohibition of unnecessary suffering and the principle of proportionality, were already established in the so-called Saint Petersburg Declaration of 1868,⁸⁹ and then so widely accepted that they have become customary rules of IHL.⁹⁰ The relevance of these principles when considering the purposes of IHL emerges clearly when assessing their content. The principle of distinction requires that ‘[t]he parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians’.⁹¹ Under the prohibition of unnecessary sufferings, ‘[t]he use of means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering is prohibited’.⁹² Last, the principle

85 ICRC, ‘What Is International Humanitarian Law?’ <https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf> accessed 21 February 2023.

86 *ibid.*

87 In this regard, it has been affirmed that ‘fundamental principles of IHL provide that armed conflict occurs when a group takes measures that injure, kill, damage, or destroy’. DeLuca (n 16) 302.

88 ICRC, Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Commentary of 2016 (n 28) para. 1.

89 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (signed 11 December 1868, entered into force 11 December 1868) 138 CTS 297 (Saint Petersburg Declaration).

90 90 The legal body composed by rules of customary IHL ‘derives from “a general practice accepted as law”’. To prove that a certain rule is customary, one has to show that it is reflected in state practice and that the international community believes that such practice is required as a matter of law’. ICRC, ‘Customary International Humanitarian Law’ (*IHL Database. Customary IHL*, 29 October 2010) <<https://www.icrc.org/en/document/customary-international-humanitarian-law-0>> accessed 21 February 2023.

91 ICRC, ‘Rule 1. The Principle of Distinction between Civilians and Combatants’ (*IHL Database. Customary IHL*) <<https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1#:~:text=international%20armed%20conflicts-,Rule%201.,not%20be%20directed%20against%20civilians>> accessed 17 April 2023.

92 ICRC, ‘Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering’ (*IHL Database. Customary IHL*) <<https://ihl-databases.icrc.org/en/customary-ihl/v1/rule70>> accessed 17 April 2023.

of proportionality establishes that '[l]aunching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited'⁹³. On one hand, these principles regulate warfare, regardless of the means to conduct such actions; on the other, they pursue aims of protection of individuals involved in wars – again, irrespective of the type of weapons employed. Consistently, it has been submitted that they should apply in cyber-wars as well.⁹⁴

In addition, the so-called Martens provides that '[u]ntil a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience'⁹⁵. Even though it dates back to 1899, the Martens Clause was considered 'an effective means of addressing the rapid evolution of military technology'⁹⁶ by the International Court of Justice in its Advisory Opinion on the legality of the threat or use of nuclear weapons issued on 8 July 1996, and the Tallinn Manual 2.0 affirmed that it 'reflects customary international law'⁹⁷. Therefore, the Martens Clause can be considered as relevant in relation to the topic at issue. Having clarified its importance, for the purpose of the present work it should be highlighted that the Martens Clause ultimately 'provides authority for looking beyond treaty law and custom to consider principles of humanity and the dictates of the public conscience'⁹⁸. This conclusion was supported by the International Law Commission⁹⁹.

Given all this, it appears that a reconceptualization of the criterion of intensity given the emergence of new means of warfare may take into consideration the protection of human rights. It is true that armed conflicts necessarily lead to a compression of human rights, however, as already recalled, IHL aims at striking a balance between military necessities and the protection of individuals. In

93 ICRC, 'Rule 14. Proportionality in Attack' (*IHL Database. Customary IHL*) <<https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14>> accessed 17 April 2023.

94 Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal* 1.

95 Convention II with Respect to the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land' (adopted 29 July 1899, entered into force 4 September 1900) Preamble (so-called Martens clause).

96 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 1996 226.

97 Schmitt (n 5) r 20 para 10.

98 Rupert Ticehurst, 'The Martens Clause and the Laws of Armed Conflict' (1997) 37 *International Review of the Red Cross* (1961-1997) 125.

99 ILC, 'Report of the International Law Commission on the Work of Its 46th Session' (2 May–22 July 1994), UN Doc A/49/10, 317.

this sense, the assessment of the intensity criterion, conducted under a flexible approach, may take into consideration whether the armed attacks compromise the enjoyment of fundamental human rights, that cannot be protected by law applicable in peacetime. This conclusion appears to be consistent not only with the ultimate and original aims of IHL, but also with the current development of international law in general. In this regard, it appears that in the last decades, human rights have gained more and more relevance, and the branches of IHL and IHRL are more and more merging, leaving the sharp separation in their application behind. These two issues are now further developed.

First, the relevant role gained by IHRL in recent years has been recognized both in practice and doctrine. The adoption of several international conventions on human rights,¹⁰⁰ and the institution of several regional courts dedicated to the protection of human rights (notably the European Court of Human Rights), prove the relevance gained by IHRL after the Second World War. Second, the different application between the two legal frameworks is not considered as blunt as in the past. It used to be submitted that IHRL and IHL were two alternative legal frameworks, IHRL being applied in peacetime, IHL in wartime. This theory, however, is not unanimously endorsed today, and an approach which takes into consideration the necessities of human beings even in case of armed conflicts is gaining more and more strength. In this sense, it is worth mentioning an excerpt by the ICTY decision on the defense motion for interlocutory appeal on jurisdiction given in the *Tadić* case: ‘the impetuous development and propagation in the international community of human rights doctrines, particularly after the adoption of the Universal Declaration of Human Rights in 1948, has brought about significant changes in international law, notably in the approach to problems besetting the world community. A State-sovereignty-oriented approach has been gradually supplanted by a human-being-oriented approach’.¹⁰¹

Besides the compatibility of the human-rights based approach to the ultimate aim of IHL and to the more and more central role of IHRL, the approach

100 Such as the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171; International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3; Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) 1465 UNTS 85; Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, entered into force 3 May 2008) 2515 UNTS 3. On a regional level, see the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221; American Convention on Human Rights (adopted 22 November 1969, entered into force 27 August 1979) 1144 UNTS 123.

101 *The Prosecutor v Dusko Tadić (Appeals Chamber, Decision on The Defence Motion for Interlocutory Appeal on Jurisdiction)* (n 45) para 97.

that takes into consideration human rights presents the flexibility required in the assessment of the elements required for a NIAC to come into existence. Given the rapid technological developments in methods of warfare we are witnessing today, this flexibility may be a quality, as it may render the approach suitable to assess the intensity criterion notwithstanding the methods of warfare employed.

Another positive aspect of this approach is that it may be consistent also with the rules on technologically developed forms of warfare. In particular, the thesis arguing that cybernetic attacks should be conceptualized on the basis of their correspondence to kinetic ones should be analyzed. In the Tallinn Manual 2.0 it is stated that '[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause *injury or death to persons* or damage or destruction to objects' (emphasis added). When the harm produced by the former corresponds to the one produced by the latter, it is possible to have a cybernetic attack.¹⁰² In addition, the notion of attack may be expanded beyond injuries and death, comprehending serious illnesses and severe mental sufferings.¹⁰³ For instance, a cyber-attack that compromises the correct functioning of a dam, thus causing a flood that kills several persons and destroys the houses in the area nearby, may be considered as reaching the level of intensity required. Similar conclusions may be reached considering the hypothesis of a dam similarly compromised by the attack of a drone. While it is true that drone attacks are kinetic in nature, it is also true that the attacks conducted employing them normally have low-intensity impacts. However, when taking into due consideration human rights, the assessment of whether the intensity criterion has been reached or not becomes possible. Using the same example, drone attacks that compromises the correct functioning of a dam may be considered as reaching the level of intensity required.

It can be concluded that the issues on the assessment of the intensity criterion required to identify the existence of a NIAC caused by the more and more widespread usage of modern, technologically advanced weapons, may benefit from the reference to a human-rights-based perspective. This is consistent not only with the ultimate purpose of IHL, but also with the general development of international law. In addition, it is also consistent with international case law. On a practical level, a human-rights-based may provide a suitable, flexible approach, apt to assess new types of armed violence, characterized by the resort to rapidly evolving means of warfare.

102 Schmitt (n 5) r 30 para 5. See also, eg, Gabriele Della Morte, *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*. (Editoriale scientifica 2018) esp. 186 ff.

103 Schmitt (n 5) r 30 para 8.

7. Conclusions

The evolution of armed violence towards the usage of more and more technologically advanced means of warfare may create problems in the application of IHL. One of the main issues regards the field of NIACs, which are, today, spread worldwide. To identify the existence of a NIAC, a minimum threshold of intensity must be reached; however, new means of warfare, e.g., attacks using drones and cyber-attacks, may never reach the level of intensity required. Of course, this may constitute a problem: if a situation of armed violence would not be considered as a NIAC, the rules and guarantees provided by IHL would not apply.

Given all this, the intensity criterion should be reconceptualized. To do so, it is necessary to examine the concept of intensity as it has been developed and interpreted up until now. In this sense, it emerges that it has not been strictly defined by both international law and practice. However, its unprecise scope does not appear as a shortcoming: on the contrary, it appears that relevant international case law left it unclear on purpose, in order to leave it enough flexibility to apply in different circumstances.

While several theories, aimed at reconceptualizing the criteria necessary for the identification of a NIAC, have been submitted, it appears that a case-by-case approach, keeping into consideration the instances of protection of human rights, should be preferred. Indeed, even though the assessment required applying this approach is lengthy and complex, the latter appears the most suitable to assess current armed violence while being consistent with IHL and international law in general, as well as apt to assess new forms of armed conflicts with new methods of warfare. However, such a flexible approach needs a stable point anyway, and the focus on the protection of human rights seems the most suitable, both because of the ultimate goal of IHL and because of the relevance gained by IHRL in recent decades.

Arguably, the reconceptualization of the criterion of intensity should be object of further studies. Indeed, two main issues emerge: first, while providing enough flexibility to be compatible with international case law on the issue, the inquiry required to evaluate whether the intensity criterion has been reached or not may be long; second, it may be submitted that the violation of not all human rights may lead to the reaching of the minimum threshold of intensity required for a NIAC to come into existence. Besides being compatible with the list included in the Tallinn Manual 2.0, this may be compatible with the widespread classification of human rights into several categories. However, given that it has been submitted that IHL should be reformulated as a whole to

accommodate new means of warfare¹⁰⁴, the issues presented may be tackled during this wider process of reconceptualization.

¹⁰⁴ See, eg, Michael N Schmitt, 'Classification of Cyber Conflict' (2012) 17(2) *Journal of conflict and security law* 245.

Autonomous Navigation and International Law: Does the Principle of Meaningful Human Control Apply at Sea?

Daniele Mandrioli

University of Milan, Italy

ORCID 0000-0002-8829-7923

DOI: 10.54103/milanoup.215.c447

Abstract

As it is commonly known, digital technologies and automation are revolutionizing maritime operations, offering significant economic and safety benefits by reducing human errors. Despite these advancements, the legal implications of Maritime Autonomous Surface Ships (MASS) have not been thoroughly explored by the international community. The present paper examines the intersection of autonomous maritime navigation and international law, specifically the principle of Meaningful Human Control (MHC). Accordingly, this study addresses whether autonomous maritime navigation falls under the principle of MHC, which mandates that Autonomous Weapon Systems (AWS) be under human control to be considered lawful under International Humanitarian Law (IHL). The paper traces the origins of the MHC debate within IHL, discussing its relevance and potential applicability to maritime navigation. It analyzes international maritime regulations, such as the United Nations Convention on the Law of the Sea (UNCLOS), which implicitly assume human involvement in navigation. However, the study argues that these regulations do not necessarily prohibit the use of MASS but highlight safety concerns that could arise from the lack of human operators on board. A significant focus is placed on the legal status of the shipmaster, a role traditionally charged with the control and responsibility of the vessel. The paper examines whether this role can be adapted to include remote or autonomous control, suggesting that the presence of a human controller, even if remote, might fulfil the MHC requirement. Fully autonomous ships, which operate without direct human oversight, raise questions about compliance with international law. The study acknowledges the challenges in defining the normative content of MHC for autonomous navigation, particularly as the degree of automation increases. It explores different

levels of human involvement, from remote control to full autonomy, and debates whether programmers of autonomous systems could be considered as fulfilling the role of shipmasters under international law. Concluding, the paper emphasizes the need for further exploration and debate on the application of MHC to maritime navigation. It suggests that while the current legal framework does not explicitly address the use of MASS, evolving interpretations and new regulations could potentially accommodate these advancements. The research underscores the importance of international consensus and regulatory adaptation to ensure the safe and lawful integration of autonomous technologies in maritime operations. From a methodological perspective, this study examines the chosen topic by proposing a systemic analysis of different regimes of international law (particularly IHL and LOS), aiming to distill the systemic relationship that may emerge from the combined observation of various branches of the international legal system.

Keywords

Autonomous Navigation, International Law, Meaningful Human Control, Maritime Autonomous Surface Ships (MASS), Shipmaster, UNCLOS, Maritime Safety, Automation

1. Introduction

As it is becoming increasingly clear, digital technologies are redefining the *ergonomics*¹ of traditional human behaviour. With specific regard to the maritime field, the process of digitalisation of information² allows the achievement of ever-increasing levels of automation, opening great opportunities for the shipping industry. Intuitively, the reduction/absence of crew on board entails a considerable reduction of costs for operators, and for consumers as well.³ In terms

1 For the purposes of this research, the science of ‘ergonomic’ is defined as the discipline ‘concerned with the understanding of the interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well being and overall system performance’. This definition is given by the International Ergonomics Association (reported in Michelle Grech, Tim Horberry and Thomas Koester, *Human Factor in the Maritime Domain* (Routledge 2008) 11).

2 In World Maritime University, *Transport 2040: Automation, Technology, Employment – The Future of Work* (World Maritime University 2019) 7, the word ‘digitalisation’ is defined as ‘the process of introducing digital components into systems and processes thereby enhancing or replacing physical components by electronic systems’.

3 In this regard, see R Glenn Wright, *Unmanned and Autonomous Ships: an Overview of MASS* (Routledge 2020), 23–27; Lucy Carey, ‘Report on BIMCO Autonomous Ships Seminar’ (NUS, Centre for Maritime Law, 2019) 14 <<https://law.nus.edu.sg/wp-content/uploads/2020/04/CML-R1901.pdf>> accessed 30 May 2024; Yewen Gu and others, ‘Autonomous Vessels: State of the Art and Potential Opportunities in Logistics’ (Discussion Paper, Institutt for foretaksøkonomi, September 2019) <<https://openaccess.nhh.no/nhh-xmlui/bitstream/>

of maritime safety, furthermore, the innovation of autonomous control sharply reduces the risk of casualties deriving from human mistakes occurring on board the ships.⁴ For these reasons, States and private entities are both investing many economic resources in developing autonomous vessels: in the last decade, the first *Maritime Autonomous Surface Ships* (MASS) have been tested and produced. The adoption of this technology is not futuristic anymore: nowadays, more than a thousand MASS navigate in the oceans.⁴

Generally speaking, the advent of digital technologies poses unprecedented juridical questions. With regard to the international legal system, in particular, it is worth noting that the protection of human rights is facing a process of evolution in order to address the menaces nested inside the digital domain.⁵ Quite similarly, the exponential rise of cyber-activities is questioning many aspects related to the law of State Responsibility and the *jus ad bellum*.⁶ Again, the unique characteristics of autonomous weapon systems (AWS) are inspiring an intense debate concerning their legitimacy under international humanitarian law.⁷

handle/11250/2612601/0619.pdf?sequence=1> accessed 30 May 2024; Agamy S Kazem and Helal Hesham, 'Autonomous Surface Ships, In View of Existing Legislation, and the Need for a New Governance' (2018) 7 *The International Maritime Transport & Logistics Conference* 30; UNCTAD, 'Review of Maritime Transport' (2018) 90–92, <https://unctad.org/system/files/official-document/rmt2018_en.pdf> accessed 30 May 2024.

- 4 As it is known, this is the most frequent origin of maritime accidents. To more in this regard, see Nora Berg, Jenni Storgard and Jouni Lappalainen, 'The Impact of Ship Crews on Maritime Safety' (Centre for Maritime Studies University of Turku, 2013) 35; Grech, Horberry and Koester (n 1) 17–18.
- 5 Ganluigi Castelli, Severino Meregalli and Ferdinando Pennarola (eds), *The Post-Digital Enterprise* (Springer 2022); Alessandro Stiano, 'Il diritto alla privacy alla prova della sorveglianza di massa e dell'intelligence sharing: la prospettiva della Corte europea dei diritti dell'uomo' (2020) 2 *Rivista di Diritto Internazionale* 511; Gabriele Della Morte, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti* (Editoriale Scientifica 2019); Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56(1) *Harvard International Law Journal* 81.
- 6 Giovanna Adinolfi, 'States' Economic Measures to Counter Cyberattacks: Disentangling Their (Il)legitimacy under International Law' (2022) 3 *Rivista di Diritto Internazionale Privato e Processuale* 513; Gabriele Della Morte, 'Limiti e prospettive del diritto internazionale nel cyberspazio' (2022) 1 *Rivista di Diritto Internazionale* 5; François Delerue, *Cyber Operations and International Law* (CUP 2020); Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31(3) *European Journal of International Law* 941; Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer 2017); Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21(3) *Journal of Conflict and Security Law* 429; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014).
- 7 Diego Mauri, *Autonomous Weapons Systems and the Protection of the Human Person* (Elgar 2022); Daniele Amoroso, *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains* (Editoriale Scientifica 2020); Wolff Heintsche von Heinegg and Robert Frau, Singer (eds), *Dehumanization of Warfare* (Springer 2018).

In this scenario, even the law of the sea is challenged by digitalisation and autonomous control: since ships may now be (fully or partially) commanded without human involvement in the decision-making loop, the international regulation on the activity of navigation must face the peculiar challenges brought by this new factual reality.⁸

That being said, however, it is worth noting that to date the legal impact of MASS has not been deeply considered by the international community.⁹ So far, the very first studies in this regard do not have the ambition to address this topic from a general perspective: quite on the opposite, the current debate is usually limited to tackling very specific and ‘hyper-technical’ issues, such as, for example, the compliance of autonomous ships with safety requirements provided by international treaty law.¹⁰ The poor size and consideration of a holistic debate on MASS are even more critical when compared to other fields of international law (such as those mentioned above), where the legal impact of digitization has already sparked wide-ranging and more comprehensive reflections.

8 For a more detailed introductive study about the rise of autonomous ships and its potential challenges in International Law, this author refers to his previous scripts in this field, which, while dealing with the same technical innovation, address different legal aspects of the topic. See Daniele Mandrioli, ‘The Rise of Autonomous Ships: Towards an Evolutionary Interpretation of the IMO Treaties on Safety of Navigation?’ (2022) 1 *Il Diritto Marittimo* 159, 163–164; Daniele Mandrioli, ‘The International Duty to Assist People in Distress at Sea: No Place for People on Board’ (2020) 26 *Humanidades & Tecnología* 77, 79–82.

9 For sake of completeness, it must be specified that a primordial debate on the legal impact of MASS has been advanced by the International Maritime organization (IMO). In particular, the IMO has published two primordial, not binding analysis, on this subject (MSC.1/Circ.1638, Outcome of the Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships (MASS), 3 June 2021; LEG.1/Circ.11, *Outcome of the Regulatory Scoping Exercise and Gap Analysis of Conventions Emanating from the Legal Committee with respect to Maritime Autonomous Surface Ships (MASS)*, 15 December 2021). These works reflect the first efforts of the international community concerning the topic here object of analysis. However, what lacks today is the establishment of a broad legal debate on autonomous navigation that goes beyond the mere maritime affairs, thus taken into account all the issue of the law of the sea adopting a holistic perspective.

10 In this regard, see, among others: Mika Viljanen, ‘How to Ensure Safe Navigation: Navigation Safety Regulation in MASS’ in Herausgegeben Von, Tafsir Matin Johansson, Jonatan Echebarria Fernández, Dimitrios Dalaklis, Aspasia Pastra, and Jon A. Skinner (eds), *Autonomous Vessels in Maritime Affairs* (Springer 2023); Henrik Ringbom, ‘Developments, Challenges and Prospects at the IMO’ in Henrik Ringbom, Erik RØsæg and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2020); Aldo Chircop, ‘Maritime Autonomous Surface Ships in International Law: New Challenges for the Regulation of International Navigation and Shipping’ in Myron H Nordquist, John Norton Moore and Ronán Long (eds) *Cooperation and Engagement in the Asia-Pacific Region* (Brill 2019) 251; Robert Veal and Henrik Ringbom, ‘Unmanned Ships and the International Regulatory Framework’ (2017) 23(2) *Journal of International Maritime Law* 100; Eric Van Hooydonk, ‘The Law of Unmanned Merchant Shipping – An Exploration’ (2014) 20 *Journal of International Maritime Law* 403.

In particular, a thought-provoking debate has arisen for what concerns the presumed emergence of a new international rule of humanitarian law – the so-called *principle of Meaningful Human Control* (MHC) – pursuant to which the use of AWS would be legitimate only if these military instruments are ‘meaningfully’ controlled by human operators.¹¹ In the past decade, the international community largely discussed the progressive development of the *ius in bello* regime in this respect, thus inspiring large-scale reflections on the intertwined relations occurring between digitization, human control, human dignity and international law.¹²

Recognizing the increasing consideration that the already mentioned topic has gained over the years, the present research aims at analogically transposing this debate into the law of the sea. Precisely, this work addresses the question of whether the activity of maritime navigation is covered by the principle of MHC and, eventually, how this rule impacts the ongoing process of digitalisation of the shipping field. From this perspective, the proposed analysis will start by briefly reconstructing the origins of the debate in its context of belonging, ie the regime of international humanitarian law (section 2). Subsequently, it will address the central issue of this work, concerning the hypothesized validity of the principle of MHC in the law of the sea. Methodologically wise, the research will first provide a systemic analysis of the most relevant international provisions implying human involvement in navigation, in order to get some knowledge about the (eventual) validity of MHC at sea (section 3). In this respect, the international rules dealing with the figure of the shipmaster, ie the individual in charge of the activity of navigation, will cover a role of paramount importance (section 4). The present study will then attempt to investigate the definition of the normative content of MHC at sea, with the aim to better understand whether and how the use of MASS complies with international law (section 5).

Before starting the proposed analysis, a last clarification is necessary. When referring to ‘MASS’, the present research avails of the definition advanced in this field by the International Maritime Organization (IMO). In the preliminary

11 Among many others, see Mauri (n 7); ICRC, ‘ICRC Position Paper on Autonomous Weapon Systems’ (2021) <www.icrc.org/en/document/icrc-position-autonomous-weapon-systems> accessed 30 May 2024; Daniele Amoroso and Guglielmo Tamburini, ‘Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues’ (2020) 1 Current Robotic Reports 187; Marta Bo, ‘Meaningful Human Control over Autonomous Weapon Systems: An (International) Criminal Law Account’ (*OpinioJuris*, 2020) <<https://opiniojuris.org/2020/12/18/meaningful-human-control-over-autonomous-weapon-systems-an-international-criminal-law-account/>> accessed 30 May 2024; Thompson Chengeta, ‘Defining the Emerging Notion of “Meaningful Human Control” in Weapon Systems’ (2017) 49 New York University International Law and Politics 833; Rebecca Crotoof, ‘A Meaningful Human Floor for “Meaningful Human Control”’ (2016) 30 International and Comparative Law Journal 53.

12 Amoroso (n 7) 4.

works of the Organization, the acronym ‘MASS’ has referred to any ship, which, ‘[...] to a varying degree, can operate independently of human interaction’.¹³ As recognized by the IMO itself, this new technology has a broad nature; potentially, many different ‘levels’ of automation could be included inside this definition. For sake of clarity, the Organization has identified four sub-categories of MASS, better specifying the types of autonomous ships existing today:

Degree one: Ship with automated processes and decision support: Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control;

Degree two: Remotely controlled ship with seafarers on board: The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions;

Degree three: Remotely controlled ship without seafarers on board: The ship is controlled and operated from another location. There are no seafarers on board;

Degree four: Fully autonomous ship: The operating system of the ship is able to make decisions and determine actions by itself’.¹⁴

In light of the above, the present research will limitedly consider the last two levels of automation – namely *remotely-controlled* and *fully autonomous MASS* –, whose navigation inspires critical thoughts concerning their presumed incompatibility with the principle of MHC, here specific object of analysis.

2. The concept of MHC in international humanitarian law

‘The exercise of control over the use of weapons, and, concomitant responsibility and accountability for consequences are fundamental to the governance of the use of force and to the protection of the human person’.¹⁵ Ten years ago, the NGO ‘Article 36’ has thus contributed to the debate on the legitimacy of AWS under international law. From that moment on, States, international organizations and scholars have largely discussed whether the use of AWS, above and beyond their compliance with the already-established principles of

13 IMO Docs. MSC 98/23 of 28 June 2017.

14 IMO RSE, 3–4. For a more detailed analysis about this classification, see Henrik Ringbom and Felix Collin, ‘Terminology and Concepts’ in Henrik Ringbom, Erik RØsæg and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2020).

15 Article 36, ‘Structuring Debate on Autonomous Weapon Systems’ (2013) <<https://article36.org/wp-content/uploads/2013/11/Autonomous-weapons-memo-for-CCW.pdf>> accessed 30 May 2024.

humanitarian law,¹⁶ should be considered 'a malum per se'.¹⁷ In a nutshell, the international community has been called to understand if the absence of human involvement in the decision-making loop introduces not only ethical concerns,¹⁸ but also legal ones, therefore prohibiting the avail of AWS by the simple fact of not complying with the so-called principle of MHC.

This innovative line of research has been set up on two cumulative steps of analysis. First, to ascertain the binding nature of this requirement it is necessary to recognize its international legal source;¹⁹ second, the eventual genesis of this rule imposes to reconstruct its normative content, in order to well define what 'meaningful human control' properly means when dealing with AWS.

As regards the first issue, scholars are quite divided upon which source of international law should be the normative ground of MHC. In the contextual absence of any conventional provision strictly dealing with AWS, some authors are of the view that a new customary rule is progressively emerging in the field of humanitarian law.²⁰ Accordingly, albeit it still lacks consistent State practice, the rise of such a popular debate, taken together with the lack of clear opposition from any national Government, could highlight the emergence of *opinio iuris* in this respect.²¹ Even the analysis of soft law instruments should be seen as evidence that the process of consolidation of a new rule of general international law, while not concluded, has at least already started.²²

16 Just to provide some examples, we refer to the renowned international principles of distinction and proportionality. To more in this regard, see, *ex multis*: Mauri (n 7) 118–175; Elliot Winter, 'The Compatibility of Autonomous Weapons with the Principle of Distinction in the Law of Armed Conflict' (2020) 69(4) *The International & Comparative Law Quarterly* 845; Thompson Chengeta, 'Measuring Autonomous Weapon Systems against International Humanitarian Law Rules' (2016) 5(1) *Journal of Law and Cyber Warfare* 63, 66; Jeroen van den Boogard, 'Proportionality and Autonomous Weapons Systems' (2015) 6(2) *Journal of International Humanitarian Legal Studies* 247.

17 Amoroso (n 7).

18 For a philosophical analysis of this issue, see Filippo Santoni de Sio and Jeroen van den Hoven, 'Meaningful Human Control over Autonomous Systems: A Philosophical Account' (2018) 5 *Frontiers in Robotics and AI* 1.

19 This paper refers to the sources of international law as listed in art 38(1) of the Statute of the International Court of Justice, ie international treaties, customary rules and general principles recognized by civilized Nations.

20 See Peter Asaro, '*Jus Nascendi*, Robotic Weapons and the Martens Clause' in Rayan Calo, A Michael Froomkin and Ian Kerr (eds), *Robot Law* (Elgar 2016); Kevin Neslage, 'Does "Meaningful Human Control" Have Potential for the Regulation of Autonomous Weapon Systems' (2016) 6 *University of Miami National Security and Armed Conflict Law Review* 151.

21 Crotoof (n 11) 53.

22 For example, the General Comment No. 3, of 2015 of the African Commission on Human and Peoples' Rights, when saying that 'Any machine autonomy in the selection of human targets or the use of force should be subject to meaningful human control', may be seen as another (timid) sign of the evolving trend that is now pervading International Humanitarian

Contrary to this position, other scholars²³ believe that, to demonstrate the binding force of the MHC requirement, it is not strictly necessary to reconstruct its customary nature; thanks to the systemic role covered by the ‘*Martens Clause*’ in case of *vacatio legis*,²⁴ even mere considerations of humanity, like those emerging from the use of AWS, may acquire a certain legal relevance. As it is known, indeed, many international humanitarian law treaties²⁵ explicitly provide that, in the lack of specific provisions, international legal subjects must anyway ensure that civilians and combatants shall always remain under ‘[...] the protection and authority of the principles of international law derived from established custom, from the *principles of humanity* and from the dictates of public conscience’.²⁶ As also noted by the International Court of Justice, this peculiar mechanism not only guarantees the applicability of human rights law in times of war, but it also allows the *ius in bello* regime to ‘keep up’ with the novelties brought by the technological military development.²⁷

Law, AfCommHPR, ‘General Comment No. 3 on the African Charter on Human and Peoples’ Rights: The Right to Life (Article 4)’ (adopted in November 2015) (General Comment No 3).

23 Among many others, see Amoroso (n 7), 161–214; Tyler Evans, ‘At War with Robots: Autonomous Weapon Systems and the Martens Clause’ (2013) 41(3) *Hofstra Law Review* 697; Asaro (n 20).

24 For a deep analysis of the peculiar relevance of the ‘Martens Clause’ in international law, *ex multis*, see: Antonio Cassese, ‘The Martens Clause: Half a Loaf or Simply Pie in the Sky?’ (2000) 11 *European Journal of International Law* 187, 188; Rupert Ticehurst, ‘The Martens Clause and the Laws of Armed Conflict’ (1997) *International Review of the Red Cross* 125; Michael Salter, ‘Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause’ (2012) 17 *Journal of Conflict and Security Law* 403; Shigeki Miyazaki, ‘The Martens Clause and International Humanitarian Law’ in Christophe Swinarski (ed), *Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet* (Martinus Nijhoff 1984); Theodor Meron, ‘The Martens Clause, Principles of Humanity and Dictates of Public Conscience’ (2000) 94(1) *American Journal of International Law* 78; Vitaliy Ivalenko, ‘The origins, causes and enduring significance of the Martens Clause: A view from Russia’ (2022) 104 *International Review of the Red Cross* 1708.

25 As it is known, the first international treaty in which this clause was inserted was the 1899 Hague Convention (II). From that moment on, the text of many other conventions provided a similar wording. Among other, see the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (AP I); the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949 (First Geneva Convention); the Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949 (Third Geneva Convention); the Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949 (Fourth Geneva Convention), and the Convention on Certain Conventional Weapons (CCW). The recognized fortune of high consideration of this clause makes scholars agree on its customary nature.

26 Preamble of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 10 April 1981 (CCW) (emphasis added).

27 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 78.

From this perspective, the fact that the use of AWS potentially excludes human involvement in military decisions may be seen as a ‘*dehumanization*’ of the targeted people: accordingly, ‘should computers be delegated the power to take targeting decisions [...], human beings at the receiving end of force would be reduced to the “zeros and ones” of a machine code’.²⁸ If one agrees with this statement, the possibility to invoke the Martens Clause in this regard would not be unreasonable; those ethical concerns that instinctively arise when thinking about AWS would be therefore elevated from a just moral ground to a normative one.

Above and beyond this preliminary issue, there remains considerable uncertainty on the normative content of the principle of MHC. In this respect, we are witnessing a complete lack of consensus within the international community. Just to provide some examples of the many different points of view existing on this matter,²⁹ the NGO Article 36 has stressed the necessity of always keeping a ‘[t]imely human judgement’, in order to guarantee a human ‘timely intervention’ over autonomous decisions.³⁰ Similarly, but not identically, some scholars have proposed another ‘prudential’ solution, according to which high levels of human control should always be ensured (‘Level 1: a human engages with and selects targets, and initiates any attack; [...] Level 2 a program suggests alternative targets and a human chooses which to attack’).³¹ Quite contrary to this background, instead, other scholars believe that the MHC requirement is fulfilled even in the absence of a direct involvement of a human operator in a particular engagement: if the steps of the targeting process are accurately followed, no issues would occur in this respect.³²

28 Amoroso (n 7) 181.

29 The following examples limitedly deal with doctrinal opinions stressed by scholars and NGOs. Regarding the debate among States on this issue, see the discussion of the Parties to the Convention on Certain Conventional Weapons (CCW) in November 2019, stimulated by the ‘Proposal for a Mandate to Negotiate a Legally-Binding Instrument That Addresses the Legal, Humanitarian and Ethical Concerns Posed by Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (LAWS)’ (proposed by the States of Austria, Brazil and Chile).

30 Article 36, ‘Key Elements of Meaningful Human Control’ (April 2013) <www.article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf> accessed 30 May 2024, 1.

31 Amoroso and Tamburini (n 11) 261: ‘The default policy would require that higher levels of human control (L1 and L2) should be applied, unless the given autonomous weapons system is an exception that the international community of states has agreed to handle by means of specific bridge rules allowing for lower levels of human control’.

32 Mark Roorda, ‘NATO’s Targeting Process: Ensuring Human Control over (and Lawful Use of) “Autonomous” Weapons’ in Andrew P Williams and Paul D Scharre (eds), *Autonomous Systems: Issues for Defence Policymakers* (NATO Communications and Information Agency, 2016)

As it emerges from the above cursory overview, the ‘meaningfulness’ of human control over AWS is a ‘grey area [...], full of complicated situations’.³³ The uncertainty surrounding its legal value, as well as its cryptic normative content, make this issue particularly unclear and indefinite. At the same time, however, it is precisely this ‘inherent imprecision’³⁴ that has contributed to sparking this debate within the international community. As recalled in scholarship,³⁵ indeed, in the world of international relations it is quite usual that States start facing a given topic when attracted by a ‘progressive but vague statement’³⁶ around which more concrete normative evolution may take place over time. From this perspective, the reported discussions are contributing to catalysing States’ attention to the many implications arising from the growing use of AWS in international humanitarian law.

3. Navigation, MHC and the law of the sea

Digital and automation technologies are not a prerogative of what occurs on dry land; on the very opposite, they affect the performance of almost every human activity, including maritime navigation. Accordingly, what has been reported in the previous pages inspires the specular question concerning the eventual existence of the principle of MHC (even) in the law of the sea: the following section aims precisely to investigate this issue.

The very first thing to remark here is that the international community has not already paid specific attention to the proposed topic. Unlike the above-mentioned debate on AWS, indeed, no official declaration of any State or international organization can be reported in this respect.³⁷ This fact has an important legal weight, since it highlights a certain lack of interest of States in dealing with this theme: the absence of care of States regarding MHC at sea theoretically

33 Crotoof, (n 11) 56; Jonathan Kwik, ‘A Practicable Operationalisation of Meaningful Human Control’ (2022) 11(43) *Laws* 1, 3.

34 Crotoof (n 11) 60.

35 Beyond the position of Rebecca Crotoof, see also Mauri (n 7) 243: ‘the continuing recurrence of MHC in the debate may be helpful in that it stresses the need for operationalizing the concept: this may advance the understanding of characteristics and implications of AWS from a technical standpoint, and then foster the debate within the CCW framework’.

36 Crotoof (n 11) 60.

37 Of course, this does not mean that the theme of autonomous navigation is not addressed by the international community. Beyond what already reported for what concerns the IMO’s effort in dealing with the regulation of the use of MASS, even States are wondering whether this new technology impacts on the law of the sea. In this regard, see the survey proposed to States by Comité Maritime International (CMI) in this respect (the responses of States to the questionnaire organized by the CMI are available at <<https://comitemaritime.org/work/mass/>> accessed 30 May 2024). However, in these occasions any State or international organization has specifically talked about the emergence of the principle of MHC in the law of the sea.

leads to the conclusion that no customary norm is progressively developing in this field.³⁸

Nevertheless, if this argument seems to preclude the possibility to advance the hypothesis of the emergence of a *new* international rule, this does not say anything about the eventual *pre-existence* of the MHC requirement in the law of the sea. Similarly to what was noted when dealing with the role played by the Martens clause in humanitarian law,³⁹ it may not be *a priori* excluded that even the law of the sea already provides one or more provisions, whose (evolutionary)⁴⁰ interpretation could demonstrate the implicit validity of MHC in the marine domain.

When looking at the international rules on navigation currently in force, what immediately emerges is that many of them imply and presuppose a certain human involvement in navigation. Just to provide some examples, art. 94 of UNCLOS asks States '[...] to take measures for ships flying its flag as are necessary to ensure safety at sea with regard [...] to: the *manning of ships*, labour conditions and the training of *crews* [...]'.⁴¹ Again, reg. V/14.1 of the IMO Convention for the Safety of Life at Sea (SOLAS)⁴² declares that 'all ships shall be sufficiently and efficiently *manned*'. Furthermore, rules 2 and 8 of the Convention on the International Regulations for Preventing Collisions at Sea (COLREGS)⁴³ impose on seafarers to navigate 'with due regard to the observance of *good*

38 This conclusion is based on the definition of 'progressive development' that emerges from the UNGA 'Fifth Report on Identification of Customary International Law by Michael Wood Special Rapporteur' (14 March 2018) A/CN.4/717, 8: 'the relevance of practice of international organizations to the formation and identification of customary international law; and the existence of rules of particular customary international law applying bilaterally and/or among States linked by a common cause, interest or activity other than their geographical position'. Manifestly, the absence of any debate among States and International Organizations precludes the possibility to affirm the existence of any progressive development of international law.

39 See s 2 of the present paper.

40 Concerning the concept of 'evolutionary interpretation' in International Law, see Eirik Bjorge, *The Evolutionary Interpretation of Treaties* (OUP 2014); Paolo Palchetti, 'Interpreting "Generic Terms": Between Respect for the Parties' Original Intention and the Identification of the Ordinary Meaning' in Nerina Boschiero and others, *International Courts and the Development of International Law* (Springer 2013). With specific regard to the evolutionary interpretation of law of the sea rules, see Richard Barnes, 'The Continuing Vitality of UNCLOS' in Jill Barrett and Richard Barnes (eds), *The United Nations Convention on the Law of the Sea: A Living Instrument* (British Institute of International and Comparative Law 2016) 459.

41 United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 3 (UNCLOS) art 94(3) (b) (emphasis added).

42 International Convention for the Safety of Life at Sea (adopted 1 November 1974, entered into force 25 May 1980) 1184 UNTS 2 (SOLAS), as amended. The SOLAS Convention currently has 165 States Parties, the combined merchant fleets of which constitute approximately 99.04% of the gross tonnage of the world's merchant fleet.

43 Convention on the International Regulations for Preventing Collisions at Sea (London, 20 October 1972, in force 15 July 1977) 1056 UNTS 16 (COLREGS), as amended. The

seamanship'. The same treaty also provides that 'Every vessel shall at all times maintain a proper look-out by *sight and hearing* [...]'.⁴⁴

It is a truism to say that, before the advent of digital and automation technologies, the use of ships has always implied the physical attendance of human operators on board. Since these rules were drafted decades ago – when States could not have been fully aware of the rise of this revolution – it is self-evident that they are intrinsically founded on a traditional idea of navigation. Of course, their 'old-fashioned' nature poses some regulatory barriers to the use of MASS:⁴⁵ when technological progress innovates the factual modalities of this human activity, therefore, the existing provisions risk not being completely effective anymore.⁴⁶

That being said, however, one thing is acknowledging the presence of international regulatory barriers to the use of MASS, another thing is distilling from this the principle of MHC, pursuant to which autonomous navigation should be considered unlawful *per se*. As already noted by scholars who addressed the 'twin' issue of AWS: 'to affirm that MHC is a legal requirement simply because technologies that have existed until now cannot do without human intervention would be an *apodictic argument*: it postulates precisely what it is expected to demonstrate'.⁴⁷

Accordingly, it sounds reasonable to conclude that the international provisions here analysed do not prohibit the use autonomous ships as such. When interpreting the above-mentioned rules in light of their object and purpose,⁴⁸ indeed, it emerges that their *ratio legis* is to ensure the *safety of navigation*.⁴⁹ the participation of the human element is perceived as a necessary requirement for

COLREGs Convention currently has 160 States Parties, the combined merchant fleets of which constitute approximately 99.03% of the gross tonnage of the world's merchant fleet.

44 *ibid* r 5. To more on this specific debate, see Mandrioli, 'The Rise of Autonomous Ships' (n 8) 174–176.

45 These regulatory barriers have been already advanced by scholars. Among others, see in this regard two collected volumes addressing many facets of this phenomenon: Tafsir Matin Johansson and others (eds), *Autonomous Vessels in Maritime Affairs: law and governance implications* (Springer 2023); Henrik Ringbom, 'Developments, Challenges and Prospects at the IMO' in Henrik Ringbom, Erik RØsæg and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2020).

46 Thanasis Karlis, 'Maritime Law Issues Related to the Operation of Unmanned Autonomous Cargo Ships' (2018) 17(1) WMU Journal of Maritime Affairs 119, 126.

47 Mauri (n 7) 43 (emphasis added).

48 The proposed interpretation is founded on the hermeneutical criteria codified by art 31(1) (a) of the Vienna Convention on the Law of the Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1115 UNTS 331.

49 Emmanuel Roucounas, *Facteurs privés et droit international public* (2002) 299 Recueil des Cours 9 183–84; David Anderson, 'The Roles of Flag States, Port States, Coastal States and International Organisations in the Enforcement of International Rules and Standards Governing the Safety of Navigation and the Prevention of Pollution from Ships under the UN Convention on the Law of the Sea and Other International Agreements' (1998) 2

protecting this specific interest. Therefore, the (complete or partial) absence of human operators in autonomous navigation seems to be not objectionable *per se*, but only because the use of MASS might not guarantee the same level of safety secured by traditional manned ships.⁵⁰

To better clarify this passage, an analogy may be advanced with the regulation of urban transport. In sum, it seems that the inconsistencies between autonomous navigation and the observed international norms are quite similar to those posed by new means of locomotion to the national rules of the road: albeit some regulatory barriers may certainly arise, this does not necessarily mean that innovative vehicles are illicit on their own. Of course, since new technologies change ‘the way of doing things’,⁵¹ they surely cause more or less serious legal concerns. However, to prove their unlawfulness ‘as such’, it should be demonstrated that their characterizing features are in breach of one or more norms of that given legal system. In the case of autonomous ships and international law, the search of this prohibitive rule is precisely the object of the present research, i.e. the principle of MHC and its alleged validity at sea. For the reasons mentioned before, however, it seems apodictic⁵² and not entirely convincing to affirm its pre-existence through the systemic interpretation of the above analysed rules on safety of navigation.

4. The legal status of the shipmaster and his/her role of ‘human controller’

The preliminary (and negative) conclusions that have been reached so far do not exhaust the range of possible solutions to find a normative floor for the principle of MHC at sea. Accordingly, the following pages will focus on another set of rules belonging to the law of the sea – ie the international provisions strictly dealing with the *shipmaster* – in order to understand if they may play a role with regard to the addressed topic.

Singapore Journal of International and Comparative Law 557; Philippe Boisson, *Safety at Sea: Policies, Regulations & International Law* (Bureau Veritas 1999) 137.

50 This issue (in particular with regard to the SOLAS Convention) is analyzed by Joel Coito, ‘Maritime Autonomous Surface Ships. New Possibilities – and Challenges – in Ocean Law and Policy’ (2021) 97 *International Law Studies* 259; Franck Smeele, ‘Switching of Regulatory Requirements: Flag State Exemptions as a Tool to Facilitate Experiments with Highly Automated Vessels and their Operational Implementation’ in Henrik Ringbom, Erik RØsæg and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2020); Natalie Klein and others, ‘Maritime Autonomous Vehicles: New Frontiers in the Law of the Sea’ (2020) 69(3) *International and Comparative Law Quarterly* 719, 728–29; Veal and Ringbom (n 10).

51 Ursula Franklin, *The Real World of Technology Revised Edition*, (Toronto: House Of Anansi Press 2004) 9.

52 See n 49 of this paper.

Although international law does not provide a general definition of ‘ship-master’,⁵³ it is replete with norms dealing with this maritime figure. Looking at the UNCLOS, for example, art. 94,4 (b) obliges flag States to make sure that: ‘each ship is in *the charge of a master* and officers’.⁵⁴ This is not the unique provision of the ‘Constitution of Oceans’⁵⁵ referring to this figure; accordingly, the word ‘master’ is also included in arts. 27 and 97, dealing with the allocation of criminal jurisdiction on board ships; in art 98, regulating the flag and coastal States’ duties of assistance to people in distress at sea⁵⁶ and, finally, in art 211, regarding pollution from ships. For what concerns this last-mentioned topic, then, even the International Convention for the Prevention of Pollution from Ships (MARPOL)⁵⁷ gives the shipmaster a fundamental role in the performance of documentary and reporting activities.⁵⁸

Broadening the outlook, the SOLAS sets several rules concerning the master’s duties. Accordingly, ‘The master shall be supplied with such information satisfactory to the Administration as is necessary to enable him by rapid and simple processes to obtain accurate guidance as to the stability of the ship under varying conditions of service’.⁵⁹ Again, the master has to supervise the use of survival crafts,⁶⁰ the functioning of the ship reporting system⁶¹ and visibility from the bridge.⁶² Moreover, the master shall communicate danger messages to shore operators⁶³ and assist people in distress at sea.⁶⁴ In addition, rule 2 of the COLREGs refers to the ‘master’ when dealing with the responsibility for

53 Except for Reg. I (c) of the International Convention on Standards of Training Convention (London, 7 July 1978, in force 11 July 1984) 1361 UNTS 2 (STCW), as amended, pursuant to which: ‘*Master* means the person having command of a ship’.

54 UNCLOS (n 42), art 94(4) (b) (emphasis added).

55 Remarks by T.B. (Tommy) Koh, President of the Third United Nations Conference on the Law of the Sea (1982).

56 About master’s duties to render assistance to people in distress at sea, in addition to the above-mentioned reg V/33(a), also art 10 of the International Convention on Salvage (1989) provides that: ‘Every master is bound, so far as he can do so without serious danger to his vessel, and persons thereon, to render assistance to any person in danger of being lost at sea’. International Convention on Salvage (adopted 28 April 1989, entered into force 14 July 1996) 1953 UNTS 193, art 10.

57 International Convention for the Prevention of Pollution from Ships (adopted 2 November 1973, entered into force 2 October 1983) 1340 UNTS 61 (MARPOL). To date, MARPOL has 162 States Parties, the combined merchant fleets of which constitute approximately 99% of the gross tonnage of the world’s merchant fleet.

58 See Simon Baughen, ‘Who is the master now?’, in Baris Soyer and Andrew Tettenborn (eds), *New Technologies, Artificial Intelligence and Shipping Law in the 21st Century* (Routledge 2019).

59 SOLAS (n 43), reg II-1/5-1.

60 *ibid* reg III/10.

61 *ibid* reg V/11, 7.

62 *ibid* reg V/22.

63 *ibid* reg V/31.

64 *ibid* regs V/33, V/34-1.

the control and circulation of ships.⁶⁵ Then, the Maritime Labour Convention (MLC)⁶⁶ deals with the master's role in the regulation of the labour conditions of his/her crew.⁶⁷ Finally, the International Convention on Civil Liability for Bunker Oil Pollution Damage (CLC)⁶⁸ and the Convention on Limitation of Liability for Maritime Claims (LLMC)⁶⁹

The joint reading of all these provisions offers some food for thought. In the first place, the presence of the master turns out to be a necessary legal condition for international navigation. Second, the above mentioned rules are based on the understanding that the master is the *human in charge of the ship*⁷⁰. Precisely, the common element binding these international norms is the recognition of the master as the '*magister navis*' of the ship.⁷¹ he/she is the person who exercises the final decision-making power in the course of navigation and who bears the responsibilities coming from it.⁷² This conclusion is pacifically supported by doctrine, according to which the master is the: '*natural person* who is responsible for a vessel and all things and persons in it and is responsible for enforcing the maritime laws of the flag state'.⁷³

In light of the above, it is now asked whether the international legal status of the shipmaster is somehow relevant to the present research. Unlike the regulatory provisions observed in the previous section,⁷⁴ the norms dealing with the master specifically deal with the *control of the activity of navigation*, which, as now observed, shall be necessarily *under the supervision of an individual*. At a first glance, therefore, these rules look particularly promising to demonstrate the validity of the MHC requirement at sea.

65 COLREGs (n 44) r 2.

66 Maritime Labour Convention (adopted on 23 February 2006, entered into force 20 August 2013) 2952 UNTS. To date, the treaty has been signed by 91 States, representing 91% of the world's gross tonnage.

67 *ibid* standard A2(1)(d).

68 More precisely, see International Convention on Civil Liability for Bunker Oil Pollution Damage (adopted 23 March 2001, entered into force 21 November 2008) 973 UNTS 3, art III(4).

69 See Convention on limitation of liability for maritime claims (adopted 19 November 1976, entered into force 1 December 1986) 1456 UNTS 221, art 1(4).

70 From this perspective, it is of emblematic value what provided in art. 94(4) (b) of UNCLOS (n 42), according to which: 'each ship is in *the charge of a master* [...]' (emphasis added).

71 This quotation derives from the ancient reflections of the Latin jurist Ulpianus, as reported in the Justinian Digest (D. de exercitoria actione, XIV,1).

72 Boisson (n 50) 307.

73 John Cartner, Richard Fiske and Tara Leiter, *The International Law of the Shipmaster* (Taylor Francis 2009), 86 (emphasis added). This position has been more recently confirmed by Goran Vojkovic and Melita Milenkovic, 'Autonomous Ships and Legal Authorities of the Ship Master' (2020) 8(2) Case Studies in Transport Policy 334; Johan Schelin, 'Manning of Unmanned Ships' in Henrik Ringbom, Erik RØsæg and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2020); Baughen (n 59).

74 See s 3 of the present paper.

That being said, however, it cannot be ignored that analogous critics to those that have been reported before (concerning the rules on safety of navigation) should be potentially advanced also in this case. In fact, one may say that the use of MASS without a shipmaster poses just mere ‘regulatory barriers’, certainly problematic, but not enough to infer from them the existence of the principle of MHC at sea.

Contrary to this potential conclusion, however, it is here sustained that some differences occur between the international rules on safety of navigation and those dealing with the shipmaster. Accordingly, while the former conceives the human element just as ‘an instrument’ to ensure safe navigation, the objective of the latter provisions is precisely to *give an individual the control of the ship*. The slight difference lies in the fact that, for the first set of rules, the presence of the human element is not necessarily the unique way for pursuing their rationale of ensuring safety of navigation: potentially, new technologies may guarantee the same (or better) results even without a crew on board.⁷⁵ The same cannot be said for what concerns the rules regarding the shipmaster; since their aim is to ensure a proper ‘human control’ over the activity of navigation, the eventual absence of an individual in charge of the ship appears to be something more rather than just a ‘regulatory barrier’.

As a further demonstration of this, it must be stressed (once again) that the peculiarity of the legal status of the shipmaster is his/her *responsibility*⁷⁶ over the activity of navigation. Generally speaking, it is pacific that the capacity of being accountable for a certain behaviour is a prerogative of human beings, regardless of the adopted technology. From this perspective, it is true that automation and digital technologies are posing unprecedented dilemmas concerning the idea of human responsibility.⁷⁷ Above and beyond revolutionary doctrinal thoughts –

75 As observed at the beginning of this work, the use of MASS is properly aimed at ensuring safety of navigation. In this regard, see note 3 of the present paper.

76 With the use of the word ‘responsibility’, it is not intention of this author to open to the debate on the ‘legal responsibility of the shipmaster in international law’ (to more in this sense, in particular with regard to shipmaster’s duties on assistance to people in distress at sea, see Irini Papanicolopulu, ‘The Historical Origins of the Duty to Save Life at Sea in International Law’ (2022) 24(2) *Journal of the History of International Law* 149; Felicy Attard, *The Duty of the Shipmaster to Render Assistance at Sea under International Law* (Brill 2020); Massimo Starita, ‘Il dovere di soccorso in mare e il “diritto di obbedire al diritto” (internazionale) del comandante della nave privata’ (2019) 1 *Diritti Umani e Diritto Internazionale* 5). More limitedly, it is here intended to stress the prerogative of human beings of being accountable for a certain happening.

77 In this regard, Italian authors have highlighted the deformations of the categories of thoughts ‘time’ and ‘space’ in observing the behaviours of individuals. See Gabriele Della Morte, ‘Limiti e prospettive del diritto internazionale nel cyberspazio’ (2022) 105(1) *Rivista di Diritto Internazionale* 5.

which even propose the direct responsibility of artificially intelligent machines⁷⁸ – humans remain the subjects accountable for the use of technology, and not vice versa. For this reason, the full replacement of human control with artificial intelligence systems appears to be highly problematic with regard to the duty upon States to ensure the presence of a master in charge of navigation.

In conclusion, the international rules prescribing the legal status of the ship-master result in being the most promising normative ground for invoking the validity of the principle here under analysis. In light of the above, it seems not absurd to advance that the current configuration of the law of the sea already prescribes that navigation shall be under MHC.

5. The difficult attempt to qualify the normative content of MHC for autonomous navigation

The conducted analysis did not address all the potential issues related to the topic here under study. As noted in section 2,⁷⁹ indeed, one thing is investigating the formal legal basis of MHC, and another one is comprehending its related normative content.

As anticipated in the introduction of this work, the revolution brought by MASS may assume many shapes and forms depending on the achieved level of automation.⁸⁰ Precisely, while the use of MASS of the third level is still under the control of human operators – despite they work from a remote location –, the same cannot be said in the case of MASS belonging to the fourth class of automation; by definition, these ships are able to ‘make decisions and determine actions by [themselves]’.⁸¹

For this very reason, once endorsed the thesis of the presumed validity of this principle at sea – by referring to the rules dealing with the shipmaster’s international duties –, the following pages aim at reconstructing the scope of application of this (alleged) normative prescription. Answering to this issue is of the utmost importance: depending on the different meanings potentially assigned to this locution, indeed, the use of MASS belonging to different degrees of automation may be considered internationally lawful or not.

From a theoretical perspective, if one conceives as ‘meaningful’ just the human control that is directly realized *on board* the ship, the use of both the MASS

78 Virginia Dignum, ‘Responsibility and Artificial Intelligence’ in Markus D Dubber, Frank Pasquale, Sunit Das (eds), *Oxford Handbook of Ethics of AI* (OUP 2020), 215; Bartosz Brozek and Marek Jakubiec, ‘On the Legal Responsibility of Autonomous Machines’ (2017) 25 *Artificial Intelligence and the Law* 293.

79 See s 2 of this paper.

80 In particular, see n 13 of this paper.

81 MSC.1/Circ.1638, ‘Outcome of the Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships (MASS)’ (3 June 2021) 3–4.

of the third and fourth levels would not comply with international law. On the contrary, if this term is interpreted more broadly – thus admitting that human control is ‘meaningful’ when it is carried out by a human individual, regardless of its location –, the *shore-based operator*⁸² in charge of a remotely controlled ship may be still considered as the shipmaster in charge of navigation. In light of this, the use of MASS of the third level would comply with the law of the sea, while, however, the use of fully-autonomous MASS would not fulfil this legal requirement.

From yet another angle, finally, it is not clear whether the work of code-programming the decision-making algorithms in charge of the MASS could be seen as an exercise of (meaningful?) human control over a ship; if one adheres to this interpretation, even fully autonomous navigation would be under the command of a human operator, i.e. the code-programmer of artificial intelligence systems. In other words, should this person be considered the master of the ship from an international legal perspective, the principle of MHC would be respected even in the case of MASS of the fourth level.

In the last few years, several scholars have already paid attention to the evolution of the role of the master in autonomous navigation. Albeit not reading this issue as an ‘overture to MHC at sea’, the majority of them are of the view that the legal concept of ‘shipmaster’ may be dynamically interpreted in the sense to comprehend even new forms of maritime human control, such as the activities carried out by the shore-based operator.⁸³ In a nutshell, the absence of a human individual controlling the ship *on board* would not be particularly critical: accordingly, the use of remotely-controlled MASS (third level) would comply with international law. On the other side, instead, the adoption of this position would necessarily bring to the conclusion that fully autonomous MASS would be illicit because of the absence of any human in charge of navigation, not even from shore.

What is more, some authors have gone so far as to envisage that, even in the case of fully autonomous navigation, instead, the code programmer of the

82 For a legal analysis concerning this new maritime figure, see Luca Ancis, ‘Navi pilotate da remoto e profili di sicurezza della navigazione nel trasporto di passeggeri’ (2019) 32(2) *Diritto dei Trasporti* 437; Umberto La Torre, ‘Navi senza equipaggio e *Shore Control Operator*’ (2019) 2(2) *Diritto dei Trasporti* 497.

83 Gabriele Asta, ‘Navi-drone e obbligo di internazionale di prestare soccorso in mare’ (2021) 1 *Rivista del Diritto della Navigazione* 243; Baughen (n 59); Natalie Klein, ‘Maritime Autonomous Vehicles within International Law Framework to Enhance Maritime Security’ (2019) 95 *International Law Studies* 244, 265; Paul Pritchett, ‘Ghost ships: Why the law should embrace unmanned vessel technology’ (2016) 40 *Tulane Maritime Law Journal* 197, 209; Comité Maritime International, ‘CMI International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework’ (Position Paper, 2018) <<https://comitemaritime.org/wp-content/uploads/2018/05/CMI-Position-Paper-on-Unmanned-Ships.pdf>> accessed 30 May 2024, 1. On the opposite advice, see Schelin (n 73) 276; Van Hooydonk (n 10) 410.

decision-making algorithms should be legitimately considered the shipmaster in charge of the ship.⁸⁴ The eventual acceptance of this highly permissive theory would completely weaken the principle of MHC of its normative relevance; if the mere fact that a human has programmed the AI system will be sufficient to satisfy the MHC requirement, the existence (or not) of individuals in the decision-making loop would be substantially irrelevant.

At the state of the art, it is practically impossible (and maybe even useless) to understand which of these interpretations should be preferred. This is because, in the contextual lack of States' practice on this debate, there is no forecast on whether and how international legal subjects will start behaving in this regard. The contemporary age is marked by a process of *technological transition*; while new challenges are clearly visible, there is still no evidence about how States will intend to address them.

That being said, however, it must be added that the IMO is already working on a process of revision of its treaties in order to overcome some regulatory issues posed by autonomous navigation.⁸⁵ In this regard, many international rules dealing with the figure of the shipmaster should be considered.⁸⁶ Although this work of revision is not precisely aimed at defining the meaningfulness of human control over the activity of navigation, it is possible that some important novelties will come from the conclusion of this preliminary work. Very recently, the IMO Maritime Safety Committee has published the first draft the non-mandatory 'MASS Code'.⁸⁷ This document asks States to ensure the necessary presence of a human individual in charge of MASS navigation. Even considering fully autonomous ships, the MASS Code affirms that: 'the ship-owner must identify *the person responsible for managing the fully autonomous ship*, who performs all the functions and duties assigned to the ship's master by applicable international instruments and the regulations of the flag State of the autonomous ship'.⁸⁸ Where this non-binding document receives consideration from States, the

84 This solution has been hypothetically advanced by Coito (n 51) 270.

85 As already noted, the IMO has already concluded the first regulatory scoping exercises on MASS (MSC.1/Circ.1638, 'Outcome of the Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships' (MASS), 3 June 2021; LEG.1/Circ.11, 'Outcome of the Regulatory Scoping Exercise and Gap Analysis of Conventions Emanating from the Legal Committee with respect to Maritime Autonomous Surface Ships (MASS)', 15 December 2021). Next steps will be expected in the next future.

86 MSC.1/Circ.1638, 9: "[...] some common potential gaps and/or themes were regarded as high-priority issues that cut across several IMO instruments and might require a policy decision before addressing individual instruments. Among those are, for instance: .1 meaning of the terms *master*, *crew* or responsible person; .2 remote control station/centre; and .3 *remote operator designated as seafarer*" (emphasis added).

87 MSC 107/5, Development of a Goal-Based Instrument for Maritime Autonomous Surface Ships (MASS), 27 February 2023.

88 *ibid*, 5 (emphasis added).

thesis that a human operator shall exist (even from a remote location) might find more justification.

To date, since none of the prospected solutions are somehow endorsed by any State acts or declarations, the process of interpretation of MHC at sea is just a speculative operation. In stark contrast with the debate on the legitimacy of AWS – where many different State positions may be already considered⁸⁹ – the topic here analysed is still surrounded by a cryptic silence. Within this scenario, all that remains to do is to look forward to the subsequent agreements and practice of States in applying these international provisions with regard to autonomous navigation.⁹⁰ At the state of the art, therefore, the issue of when human control may be considered ‘meaningful’ at sea is an entirely open question.

6. Conclusive remarks

The way how humans interact with the phenomenological world is the focal point around which international law is built. Even though States are the primary legal subjects of the international legal system, in the final instance, international law speaks to individuals and governs their actions.⁹¹ In a nutshell, international rules are an expression of the normative power regulating human behavior at a supranational level. Once acknowledged this, it follows that, every time technological progress innovates the ‘way of doing things’,⁹² international law is subject to change. For this very reason, the technologies of digitalisation and autonomous control are bringing unexplored legal challenges.

The rise of MASS in the shipping field is a tremendous innovation. This technology revolutionizes the ergonomics of maritime human activities, undermining the common-sense perception of ‘navigation’. Intuitively, this technical advancement puts to the test the capacity of the existing norms on navigation to properly regulate the use of innovative means of maritime transport. Within this evolving scenario, the present research has limitedly focused on the unexplored topic of the potential illegitimacy of autonomous ships for the simple fact of being independent of (meaningful) human control.

⁸⁹ See s 2 of this paper.

⁹⁰ This author avails of the hermeneutical criterion as codified in art 31(3) (a) and (b) of the VLCT, pursuant to which the process of treaty interpretation takes into account ‘any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions’, and ‘any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation’.

⁹¹ Dionisio Anzilotti, *Il diritto internazionale nei giudizi interni* (Zanichelli 1905) 52. More recently, this approach to the study of international law has been proposed by Antonio Cançado Trindade, *International Law for Human Kind. Towards a New Jus Gentium* (Martinus Nijhoff Publishers 2020).

⁹² See n 51.

To date, one may wonder whether the above analysis is a useful exercise. As noted in the previous pages, indeed, the chosen topic is an entirely ‘uncontaminated field’: as far as this author knows, no State or International organization has already tackled it. This fact in itself precludes the possibility to reach positive solutions to the proposed legal questions. Unlike the field of humanitarian law,⁹³ in fact, there still is no evidence of the progressive development of any new rule in the law of the sea about MHC. Furthermore, even if the binding nature of this requirement may be presumably reached through the evolutionary interpretation of the rules on shipmaster’s duties (section 4), also this line of argument does not provide a useful indication about its normative content, thus leaving this field open to any possible scenario (section 5).

In synthesis, the above conducted analysis has led to more questions rather than answers. Their relevance, however, should not be underestimated.

First of all, the (hoped) prosecution in the study of MHC at sea looks particularly promising to generally increase *State attention on autonomous ships and their international legal implications*. When dealing with the ‘twin’ debate on AWS, it was noted that the indefinite nature of MHC is somehow encouraging States to join this discussion without excessive fears:⁹⁴ for the same reason, it should not be excluded that a similar result may occur even in this respect. Moreover, if one looks at the historical evolution of the law of the sea in the last decades, this would not be the first time that States started facing new themes when particularly attracted by a ‘vague but inspiring’ principle. As a clear example of this, it is well known that the final process of negotiation of the UNCLOS⁹⁵ was strongly influenced by the indefinite and (at the time) futuristic concept of the *common heritage of humankind*.⁹⁶ From this perspective, therefore, even ‘just

93 As it has been noted in s 2, this thesis is progressively gaining some consideration in scholarship. In particular, see n 20.

94 See n 35.

95 UNCLOS (n 42). To date, 168 States are parties to the present treaty.

96 As known, the first step of the third and definitive process of negotiation on the Convention on the Law of the Sea (UNCLOS III) started with the renowned speech of the Maltese Ambassador Arvid Pardo, during the United Nations General Assembly, Twenty-second session, 1 November 1967. This principle is now codified in art 136 of UNCLOS. For an in-depth study on the principle of the common heritage of humankind, among many others, see María Fernanda Millicay, ‘The Common Heritage of Mankind: 21st Century Challenges of a Revolutionary Concept’ in Lilian del Castillo (ed), *Law of the Sea, From Grotius to the International Tribunal for the Law of the Sea* (Brill 2015), 272; Rudiger Wolfrum, ‘Common Heritage of Mankind’ (2009) Max Planck Encyclopedia of International Law; Markus Schmidt, *Common Heritage or Common Burden? The United States Position on the Development of a Regime for Deep Seabed Mining in the Law of the Sea Convention* (OUP 1989). Albeit this author is conscious that the official terminology provided by UNCLOS uses the word ‘mankind’, a more recent approach prefers to use the gender-balanced expression ‘humankind’. For a detailed analysis about gender implications in the regime of the law of the sea, see Irini Papanicolopulu (ed), *Gender and the Law of the Sea* (Springer 2019).

speculative' reflections about the principle of MHC at sea may potentially contribute to increasing the attention of the international community regarding the phenomenon of autonomous navigation.

Above and beyond this reflection, a final consideration seems to be inspired by what discovered in the course of this work. If until today the concept of MHC has been limitedly observed concerning AWS, this research has suggested the possibility to broaden the scope of this study beyond the regime of international humanitarian law. As noted in the previous pages, indeed, even the law of the sea appears to be challenged by the rise of digital technologies. What is more, these could not be the unique two fields of law in which the concept of MHC acquires a certain relevance in the contemporary age: since digital technologies are contributing to redefining the ergonomics of almost every human activity, every international legal regime may be potentially challenged by the progressive development of this principle. For this reason, it looks particularly interesting to start conceiving the debate on MHC not just as a niche topic of humanitarian law (or of the law of the sea), but as a new issue regarding the international legal system as a whole.

In a nutshell, if it is true that international law, like any other set of rules, is necessarily founded on the 'the way of doing things', the rise of a new paradigm of human behaviour, such as the use of automation, introduces new and *general* questions of international law, which as such deserves to be addressed.

PART 2: THE PRIVATE SPHERE OF DIGITALIZATION

SECTION 1 – CROSS-BORDER BUSINESS TRANSACTIONS

Automated vehicles, tort liability and Private international law

*Raúl Lafuente Sánchez**

University of Alicante, Spain

ORCID 0000-0002-0348-2530

DOI: 10.54103/milanoup.215.c448

Abstract

Studies of, and research on, automated vehicles are currently underway, and their commercialisation will become a reality over the next years. Thus, the application of Artificial Intelligence (AI) to automated vehicles raises very important challenges from the regulatory point of view and, in particular, from the perspective of private international law rules. The introduction of automated vehicles will contribute to the gradual decrease in the liability of drivers involved in cross-border traffic accidents versus that of producers and operators of the AI systems installed in these vehicles. Consequently, there is a paradigm shift from the regime of the fault-based liability of the driver to that of the strict liability for damage caused by defective products. This shift will directly affect the application of the rules of private international law in order to determine the applicable law in cases of tort liability. This paper analyses the EU legislative initiatives on AI and civil liability and its compatibility with the rules of private international law applicable to tort liability arising from cross-border road traffic accidents involving automated vehicles. Methodology used: The object of my research is international by its very nature: the cross-border traffic accidents and the applicable rules of Private international law applying to determine the jurisdiction of national courts in the EU and the applicable law. Therefore, the methodology of my research work relies on interdisciplinary legal methodologies which will allow me to focus the legal problems from a conventional, institutional and domestic legal perspective – international conventions, European Union legislation and domestic rules – and to provide a comparative study of the matters analyzed.

Keywords

Artificial Intelligence, Automated vehicles, Tort liability, Conflict of Law rules

1. Introduction

One of the most prominent examples of the positive effects that Artificial Intelligence (AI) systems can have on our lives is their application in the motor vehicle sector, which will turn vehicles into AI-controlled machines or robots designed to perform the function of driving in an automated way. The major car manufacturers – Audi, BMW, Ford, GM, Honda, Mercedes, Nissan, Tesla, Toyota, Volkswagen and Volvo – have been working on this project for some time now, along with leading software development companies such as Google and Apple.

Undoubtedly, the introduction of this type of vehicle, as a clear example of the so-called Internet of Things (IoT), will increase the safety, efficiency and mobility of people and will contribute in a very positive way to the reduction of traffic accidents and victims that these collisions generate every year.¹ On most occasions, these can be attributed to human failures, to errors caused by the driver's emotional or physical state, or to driver negligence, either due to distractions, the effects of drugs or alcohol, drowsiness, inappropriate speed, or the use of mobile phones.²

However, the introduction of new technologies into our society also poses enormous legal challenges, not only in terms of regulation but also of liability, privacy and intellectual property not to mention ethical and moral issues. Accordingly, in the field of non-contractual liability of drivers involved in a cross-border traffic accident, we can be faced with two very different scenarios.

In the first scenario AI and human action interact and operate simultaneously that is to say, the level of automation is not total. Then, the person is still responsible for supervising the vehicle and is obliged to take control of it when required by the software. It means that the driver will still be responsible.

The second scenario takes place when driving is fully autonomous and the occupant has no active role or control over the vehicle. It will then be

1 *Associate Professor of Private International Law, University of Alicante (Spain), raul.lafuente@ua.es This article was partially written during my stay as Visiting Scholar at the Maastricht European Private Law Institute, Maastricht University, The Netherlands, in 2022. The research has been carried out in the framework of the ACIE (UA22) Project, funded by the University of Alicante, Office of the Vice President of Research, R&D+i.

According to a study by the consultancy KPMG, autonomous vehicle technology could reduce accidents by up to 80% by 2040. See, KPMG 'Marketplace of change: Automobile insurance in the era of Autonomous Vehicles' (White Paper 2015) <<https://assets.kpmg/content/dam/kpmg/pdf/2016/06/id-market-place-of-change-automobile-insurance-in-the-era-of-autonomous-vehicles.pdf>> accessed 31 March 2023.

2 According to data provided by the World Health Organization (WHO) in June 2021, approximately 1.3 million people die each year as a result of road accidents. In addition to the human tragedy that this represents, these accidents cost most countries 3% of their gross domestic product <<https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries>> accessed 31 March 2023.

questionable whether some responsibility can be attributed to the driver for a possible accident caused by the vehicle they are occupying; on the contrary, the driver would be exempt from responsibility as they would no longer be liable for any fault or negligence.

2. AI systems, automated vehicles and private international law

2.1. Jurisdiction: *The Brussels I-bis Regulation*

The jurisdiction of the EU courts will vary depending on the Member State where the offender is domiciled, where the accident takes place and where the vehicle is registered. So, it is necessary to analyse whether the currently applicable rules of private international law to non-contractual liability are appropriate to regulate situations arising from the involvement of autonomous vehicles in cross-border accidents.

Given that Regulation Brussels I-bis³ does not contain specific rules to determine the jurisdiction in cases of cross-border traffic accidents, the same vacuum will continue to exist with regard to determining the jurisdiction in cases where automated vehicles are implied.

This means that the forum of the defendant's domicile,⁴ where the defendant is located in the territory of the European Union, will be the competent court for claims brought against the driver, the owner, the manufacturer or the company that developed the software of the automated vehicle that caused the accident. For the purpose of determining the domicile of a natural person, the court shall apply its domestic law⁵ whereas the domicile of a legal person shall be deemed to be established at the place where its statutory seat, central administration or principal place of business is located.⁶

Similarly, in certain circumstances, the courts of a Member State other than that of the defendant's domicile may also have jurisdiction. Thus, in the field of claims for damage caused by automated vehicles, the place where the harmful event occurred or may occur is of particular interest since, in such cases, the courts of that Member State may have jurisdiction.⁷ Therefore, a double forum – *locus damni* and *locus actus* – would apply. In such cases, it will be possible to

3 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L 351/1 and subsequent amendments.

4 Art. 4 Brussels I-bis Regulation.

5 *ibid* art 62.

6 *ibid* art 63.

7 *ibid* art 7((2)).

sue before the courts of the Member State where the harmful event occurred or may occur, provided that direct damage is involved.⁸ Where such a liability claim arises from an act giving rise to criminal proceedings, the court hearing such proceedings will also have jurisdiction.⁹

In addition, the special rules governing jurisdiction in matters relating to insurance should be taken into account because, as is currently the case, the obligation to insure all vehicles registered in the EU will have to be extended to automated vehicles. In consequence, a distinction must be made when the claim is brought by the insurance company against the policyholder, the insured or the beneficiary of the insurance. In such cases, the competent courts will be those of the defendant's domicile in the European Union.¹⁰

Nonetheless, where the claim is brought against the insurer (or co-insurer) domiciled in a Member State, the Brussels I-bis Regulation provides for different forums: firstly, the defendant's domicile;¹¹ secondly, the courts of the place where the harmful event occurred;¹² and thirdly, the courts of the Member State in which the policyholder, the insured or a beneficiary are domiciled (*forum actoris*),¹³ as the Brussels I-bis Regulation provides for the possibility that the injured party can bring proceedings directly against the insurer, provided that such proceedings are possible.¹⁴

Finally, the Regulation also provides for the parties' freedom of choice and allows them to agree the jurisdiction of a Member State's court (*prorogatio fori*) within the limits and under the conditions laid down in the Regulation itself.¹⁵

2.2. Applicable law

Rome II Regulation¹⁶ coexists with the application of two international conventions adopted at the Hague Conference: the 1971 Hague Convention on the Law Applicable to Road Traffic Accidents¹⁷ and the 1973 Hague Convention on the Law Applicable to Product Liability.¹⁸

8 Case C-21/76 *Handelskwekerij Bier v Mines de Potasse d'Alsace* [1976] ECR 01735; and Case C-220/88 *Dumez France and Others v Hessische Landesbank and Others* [1990] ECR I-00049.

9 Art 7(3) Brussels I-bis Regulation.

10 *ibid* art 14(1).

11 *ibid* art 11(1)(a).

12 *ibid* art 12. This forum corresponds to that provided for in Brussels I-bis Regulation, art 7(2)

13 *ibid* art 11(1)(b).

14 *ibid* art 13(2) in relation to art 10, 11 and 12. As far as injured parties are concerned, Case C-463/06 *FBTO Schadeverzekeringen* [2007] ECR I-11321.

15 Brussels I-bis Regulation, arts 25-26.

16 Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L199/40.

17 Convention on the Law Applicable to Traffic Accidents (adopted 4 May 1971, entered into force 3 June 1975) (hereafter, 1971 Hague Convention).

18 Convention on the Law Applicable to Products Liability (adopted 2 October 1973, entered into force 1 October 1977) (hereafter, 1973 Hague Convention).

2.2.1 The Rome II Regulation

The Rome II Regulation lays down uniform rules to determine the law applicable to non-contractual obligations and therefore will apply to determine the law applicable to liability arising from cross-border traffic accidents and defective products. The Regulation ensures the proper functioning of the internal market and guarantees the conflict rules in force in the Member States to designate the same national law irrespective of the EU court before which the dispute is brought.¹⁹

The universal nature of this instrument ensures that the law designated by it is applicable even if it is not the law of a Member State.²⁰ Meanwhile, the exclusion of *renvoi* facilitates the predictability of the applicable law and makes it possible to mitigate the use of *forum shopping*.²¹

a) Liability arising from cross-border traffic accidents

In the field of cross-border traffic accidents, it will not be very common for the parties to agree on the law applicable, since they will not always be known to each other in advance. However, they may choose the law after the event that gives rise to the damage has occurred (that is to say, the accident);²² or if the agreement has been freely negotiated before the event giving rise to the damage has occurred, when it is required that the parties will have previously carried out (or are carrying out) a commercial activity.²³ In both cases, the choice may be made expressly or be implied from the circumstances of the case.²⁴

This solution provided for by the Rome II Regulation could be very useful for certain contracts relating to automated vehicles, because it would allow the parties in a contractual relationship to choose the applicable law even in cases of non-contractual liability arising from the contractual relationship, but not vis-à-vis third parties, such as the victims of the accident.

That said, it should be noted that party autonomy has two limitations: firstly, the observance of the provisions of the law (which cannot be derogated from by agreement) of the country in which the elements relevant to the situation at the time when the event giving rise to the damage occurred are located; and secondly, the provisions of Community law, as implemented in the Member State of the forum (which cannot be derogated from by agreement) where all the elements relevant to the situation at the time of the accident are located in one or more of the Member States.²⁵

19 Recital n 6 Rome II Regulation.

20 *ibid* art 3.

21 *ibid* art 24, which excludes the *renvoi*.

22 *ibid* art 14(1)(a).

23 *ibid* art 14(1)(b).

24 *ibid* art 14(1), second para.

25 *ibid* art 14(2) and 14(3).

On the other hand, the Regulation does not provide for specific rules governing non-contractual liability. Hence, the general rule will apply, that is to say, the law of the country in which the damage occurs, ie the traffic accident, irrespective of the country in which the event giving rise to the damage has occurred, and irrespective of the country or countries in which the indirect consequences of that event occur.²⁶

This rule will not apply where the person claiming to be liable and the injured party have a common habitual residence at the time when the damage occurs. In such cases, the law of the country of the common habitual residence applies.²⁷

Likewise, the Regulation provides that, where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that in which the event giving rise to the damage occurred or in which the parties – the victim and the tortfeasor – are habitually resident, the law of that other country shall apply.²⁸

Apart from this, the court that has jurisdiction could apply its own law (*lex fori*) and refuse the application of the law designated by the Rome II Regulation, but only if such an application is manifestly incompatible with the public policy of the forum.²⁹

b) Liability arising from defective products

Once automated vehicles are put on the roads, particular attention should be paid to product liability issues that may affect these vehicles. It should be borne in mind that, until now, the cornerstone of liability in this type of accident has been the human factor – the driver's fault or negligence – whereas, with the introduction of automated vehicles, other objective aspects determined by the interaction of technology and AI will come into play.

In this sense, product liability is subject to special conflict rules in the Rome II Regulation.³⁰ Despite this, the Regulation does not include a definition of the term 'product'. It is therefore necessary to turn to the provisions of Directive 85/374/EEC on liability for defective products³¹ and to consider limiting its

26 *ibid* art 4(1). With regard to the interpretation of the place where the damage occurs, we have to refer to the CJEU doctrine and the interpretation of art 7(2) of the Brussels I-bis Regulation, due to the coherence that must be guaranteed in the application of both instruments. See Rome II Regulation, recital n 7.

27 *ibid* art 4(2).

28 *ibid* art 4(3).

29 *ibid* art 26.

30 *ibid* art 5.

31 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member states concerning liability for defective products [1985] OJ L210/29 (Directive for Defective Products).

scope to movable property³² or, in contrast, to advocate for a broader definition of the term, which would be desirable in order to include in its scope intangible products such as software, which will be an important element in the development of AI in automated driving.³³

At the same time, it has to be mentioned that, despite the fact that Art 5 of the Rome II Regulation includes in its title the term ‘defective products’, its wording refers to non-contractual obligations arising out of damage caused by a product, without distinguishing in this case about its possible defectiveness. An extensive interpretation of the Regulation could lead to the argument that it includes both defective and dangerous products, in that sense defending the application of these conflict rules to technological products that are part of AI and automated driving because there is a potential risk involved, eg the damage caused by the software installed in an autonomous vehicle.³⁴

In identifying the applicable law, the Rome II Regulation sets up a complex system of cascade connections: first, the law of the country of the common habitual residence of the person claimed to be liable and the injured party;³⁵ second, in the absence of a common habitual residence of the parties, the law of the country of the victim’s habitual residence at the time of the damage, if the product was marketed in that country (international stream of commerce rule);³⁶ third, the law of the country in which the product was acquired, if it was marketed there;³⁷ and failing that, fourth, the law of the country in which the damage occurred, if the product was marketed in that country.³⁸

However, the law of the country in which the person claimed to be liable has his habitual residence shall apply if he could not reasonably foresee the marketing of the product, or a product of the same type, in one of the above-mentioned countries.³⁹

32 Peter Huber and Martin Illmer, ‘International Product Liability. A Commentary on Article 5 of ‘The Rome II Regulation’, (2007) 9 Yb PrIL 31,37–38; and Peter Stone, ‘Product Liability under the Rome II Regulation’ in John Ahern and William Binchy (eds), *The Rome II Regulation on the law applicable to non-contractual obligations: a new international litigation regime* (Martinus Nijhoff Publishers 2009) 175, 181.

33 Richard Plender and Michael Wilderspin, *The European Private International Law of Obligations* (3rd edn, Sweet & Maxwell, Thomson Reuters 2009) 551; and Marek Swierczynski and Lukasz Żarnowiec, ‘Law applicable to liability for damages due to traffic accidents involving autonomous vehicles’, 14 Masaryk University Journal of Law and Technology [2020] 177, 186.

34 Andrew Dickinson, *The Rome II Regulation: The law applicable to non- contractual obligations* (OUPUP 2008), 370; and Martin Illmer, ‘The New European Private International Law of Product Liability—Steering Through Troubled Waters’, 73 RabelZ [2009] 269, 281–282.

35 Rome II Regulation, art 5.1 which refers to art. 4(2).

36 *ibid* art 5(1)(a).

37 *ibid* art 5(1)(b).

38 *ibid* art 5(1)(c).

39 *ibid* art 5(1), last para.

Finally, the Regulation provides for the principle of manifestly closer links to apply the law of the country which is manifestly more closely connected with all the circumstances of the case.⁴⁰

2.2.2 *The Hague Convention of 1971 on the law applicable to road traffic accidents*

According to art 28 of the Rome II Regulation, the 1971 Hague Convention on the Law Applicable to Road Traffic Accidents prevails over the general rule provided for in art 4 of the Regulation, and will be applicable by the courts of the Member States which are parties to this Convention.⁴¹ The Convention has a universal character, so it shall be applied even if the designated law is not that of a Contracting State, and its application will not depend on any requirement of reciprocity.⁴²

Regarding the scope of application, the 1971 Hague Convention excludes 'the liability of manufacturers, sellers or repairers of vehicles'.⁴³ Nevertheless, this does not mean that it cannot apply to manufacturers of components, such as software installed in the autonomous vehicles involved in cross-border traffic accidents.⁴⁴

The Convention establishes as a basic principle the *lex loci delicti*, that is to say the application of the internal law of the State where the accident occurred.⁴⁵ However, it includes some exceptions to this principle depending on the number of vehicles involved in the accident and other circumstances.

Firstly, where only one vehicle is involved in the accident and it is registered in a State other than that where the accident occurred, the law of the State of registration of the vehicle shall apply for the purpose of determining liability in three cases: towards the driver, the keeper, the owner or any other person having a right in the vehicle, irrespective of their habitual residence;⁴⁶ towards the victims travelling as passengers, if they had their habitual residence in a State other than that in whose territory the accident occurred;⁴⁷ and towards the victims who were at the scene of the accident outside the vehicle, if they had their habitual residence in the State in which the vehicle was registered.⁴⁸

40 *ibid* art 5(2).

41 At the moment twenty-one States are part of the Convention; thirteen of them Member States of the EU: Austria, Belgium, Croatia, Czech Republic, France, Latvia, Lithuania, Luxembourg, Poland, Slovakia, Slovenia, Spain and The Netherlands.

42 1971 Hague Convention, art 11.

43 *ibid* art 2(1).

44 Some authors find it difficult to justify the distinction between vehicle manufacturers and component manufacturers. Marek Swierczynski and Lukasz Żarnowiec, 'Law applicable to liability' (n 33) 182.

45 1971 Hague Convention, art 3.

46 *ibid* art 4(a), first para.

47 *ibid* art 4(a), second para.

48 *ibid* art 4(a), third para.

Secondly, where the accident involves two or more vehicles, an exception to the principle of *lex loci delicti* shall apply, and the law of the State of registration shall apply, provided that these vehicles were registered in the same State.⁴⁹

Thirdly, where the accident involves one or more persons (either as perpetrators or victims) outside the vehicle or vehicles at the place of the accident, the derogation from the principle of *lex loci delicti* will apply only if all those persons are habitually resident in the State in which the vehicle or vehicles are registered.⁵⁰

Fourthly and last, it should be borne in mind that, when vehicles not registered or registered in several States are involved in the accident, the conflict rule will not be the law of the State of registration, but the internal law of the State in which they are habitually stationed. The same rule applies in cases where neither the owner, nor the keeper, nor the driver of the vehicle had, at the time of the accident, his habitual residence in the State of registration of the vehicle.⁵¹

Although the 1971 Hague Convention does not provide for the possibility of the parties choosing the law applicable to the dispute, submission may also be made by the parties after the event giving rise to the damage has occurred, according to art 14 of the Rome II Regulation. If they do so, freedom of choice will prevail over the conflict rules of the 1971 Hague Convention, even if the doctrine is not unanimous regarding whether party autonomy will make it possible to exclude the application of the Convention in favour of the State law chosen by the parties.⁵²

2.2.3 *The Hague Convention of 1973 on the law applicable to product liability*

In the same way, the application of the Convention prevails over the Rome II Regulation, in particular its art 5⁵³ (which identifies the law applicable to non-contractual obligations arising out of damage caused by defective products) and shall be applied on a preferential basis by the courts of the Member States which are contracting parties to this Convention.⁵⁴ This Convention also has a universal character, and its application will not depend on any requirement of reciprocity.⁵⁵

As to the relationship between autonomous vehicles and non-contractual liability, the Convention is of great relevance for the following reasons: first,

49 *ibid* art 4(b).

50 *ibid* art 4(c).

51 *ibid* art 6.

52 Thomas Kadner Graziano, 'The Rome II Regulation and the Hague Conventions on Traffic Accidents and Product Liability—Interaction, conflicts and future perspectives' (2008) *Nederlands Internationaal Privaatrecht*, 425.

53 Rome II Regulation, art 28.

54 At the moment, eleven States are part of the Convention; seven of them Member States of the EU: Croatia, Finland, France, Luxembourg, Slovakia, Spain and The Netherlands.

55 1973 Hague Convention, art 11.

because the 1971 Hague Convention on the Law Applicable to Road Traffic Accidents excludes from its material scope the liability of manufacturers, sellers or repairers of vehicles that may be involved in cases of autonomous driving; second, because, at EU level, legislative harmonisation in the area of product liability has only been partially carried out through Directive 85/374/EEC, which is now in the process of being revised; and third, because it establishes a complex system of conflict rules on the basis of different connecting factors that do not correspond to those provided in art 5 of the Rome II Regulation where product liability is regulated.

Despite the fact that the Convention does not provide for party autonomy, the parties may also choose the law applicable to the dispute on the basis of art 14 of the Rome II Regulation, which would apply in these cases in the absence of regulation in the Convention.⁵⁶

As far as the conflict rules are concerned, it establishes the habitual residence of the person directly suffering damage as connecting factor. Thus, the law of the State where the person directly harmed has his habitual residence will apply, provided that one of the following conditions is met: the State of the habitual residence is the principal place of business of the person claimed to be liable, or the place where the product was acquired by the person directly suffering damage.⁵⁷

Where these requirements are not met, the *lex loci damni* principle shall apply consequently, the internal law of the State of the place of injury, if that State is also the place of the habitual residence of the person directly injured, or the principal place of business of the person claimed to be liable, or the place where the product was acquired by the person directly injured.⁵⁸

In turn, where the conflict rules set out above do not apply, the applicable law shall be the law of the State where the principal place of business of the person claimed to be liable is located, although in this case the Convention allows the plaintiff to base his claim on the domestic law of the State in whose territory the damage occurred.⁵⁹

Lastly, it should be noted that neither the *lex loci damni* principle nor the habitual residence connecting factor shall apply if the person claimed to be liable establishes that they could not reasonably have foreseen that the product,

56 Thomas Kadner Graziano, 'Cross-border Traffic Accidents in the EU– the Potential Impact of Driverless Cars' (European Parliament – Directorate-General for Internal Policies of the Union, 2016) 27, <[https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU\(2016\)571362_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU(2016)571362_EN.pdf)> accessed 31 March 2023.

57 1973 Hague Convention, art 5.

58 *ibid* art 4.

59 *ibid* art 6.

or their own products of the same type, would be made available in that State through commercial channels.⁶⁰

3. A European Union approach to Artificial Intelligence

3.1. The European Parliament Resolution 2020, with recommendations to the Commission on a civil liability regime for AI

In its Resolution of 20 October 2020,⁶¹ the European Parliament called on the Commission to submit a Proposal for a Regulation on civil liability for the operation of AI systems, in order to harmonise the laws of Member States and to prevent the misuse of AI systems and regulatory fragmentation in national laws (hereafter, European Parliament Resolution 2020).⁶²

The idea of a uniform legal framework is based on the importance of civil liability,⁶³ as well as on the need to specifically review and adapt existing regimes to the new risks arising from using AI systems to ensure compensation for persons suffering personal injury or damage to property. AI systems, when they carry high inherent risks and act in an automated way, potentially endanger the general public and pose significant legal challenges to existing liability regimes. These challenges include proof of causation for the purpose of claiming compensation, as it will not always be easy to determine who controls the risk associated with the AI system; risks arising from connectivity between AI systems themselves; machine learning of AI systems; and cybersecurity breaches through hacking or hacking.⁶⁴

Thus, the Resolution recognises the need to guarantee injured parties a level of protection similar to that which currently operates when an AI system is not involved. To achieve this objective, it refers to the insurance of these systems and the guarantee of effective access to the courts in the case of a dispute.⁶⁵ It also sets out rules for the civil liability claims of natural and legal persons

⁶⁰ *ibid* art 7.

⁶¹ European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL) (2021/C 404/05) [2021] OJ C 404.

⁶² *ibid* points 2, 3 and 5.

⁶³ *ibid* para A, which provides: ‘whereas the concept of “liability” plays an important double role in our daily life: on the one hand, it ensures that a person who has suffered harm or damage is entitled to claim and receive compensation from the party proven to be liable for that harm or damage, and on the other hand, it provides the economic incentives for natural and legal persons to avoid causing harm or damage in the first place or price into their behaviour the risk of having to pay compensation’.

⁶⁴ *ibid* para H and I, and point 14.

⁶⁵ *ibid* para J.

against operators of AI systems,⁶⁶ that is to say, persons who have suffered damage or harm caused by a device or process governed by an AI system, as long as they are not its operators.⁶⁷

Therefore, the Resolution's point of departure is an approach based on the generation or management of the risk caused by the use of these AI systems, despite the fact that it does not include rules for manufacturers but for operators who exercise control over the risks inherent in the use of AI systems. In this context, to adapt the regulatory legal framework of civil liability arising from AI systems, the Resolution defines some key concepts as 'automated decision-making',⁶⁸ or 'AI systems'.⁶⁹

As a matter of private international law, the European Parliament Resolution 2020 includes a unilateral conflict rule stating that the Regulation applies:

On the territory of the Union where a physical or virtual activity, device or process driven by an AI-system has caused harm or damage to the life, health, physical integrity of a natural person, to the property of a natural or legal person or has caused significant immaterial harm resulting in a verifiable economic loss.⁷⁰

In other words, the Regulation introduces the *lex loci damni* criterion.

3.2. The Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI

Considering the benefits of the use of AI and the risks posed by the use of this new technology, the European Commission submitted a Proposal for a Regulation laying down harmonised rules in the field of AI on 21 April 2021.⁷¹ This was the first-ever legal framework for AI adopted by the European Commission, and it establishes a horizontal legal scheme and incorporates a set

66 *ibid* text of the Proposal requested, art 1.

67 *ibid* art 3(h) which reads as follows: "affected person" means any person who suffers harm or damage caused by a physical or virtual activity, device or process driven by an AI-system, and who is not its operator'.

68 *ibid* para G, which provides that: "automated decision-making" involves a user delegating initially a decision, partly or completely, to an entity by way of using software or a service; whereas that entity then in turn uses automatically executed decision-making models to perform an action on behalf of a user, or to inform the user's decisions in performing an action'.

69 *ibid* art 3(a) which defines AI system as 'a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, *inter alia*, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals'. This definition contrast with that included in AI Act, art 3(1).

70 *ibid* art 2(1).

71 Commission, 'Proposal for Regulation of the European Parliament and of the Council of the EU laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)', COM (2021) 206 final (Proposal for the AI Act).

of international norms and standards in order to ensure the safe and lawful use and application of new technologies in the EU market, as well as respect for EU fundamental rights and principles.

Finally, on 21 May 2024, the Council gave final green light to the first world-wide rules on AI (hereafter, AI Act), which is expected to apply two years after its entry into force, it is to say, in 2026.

The Proposal regulates the requirements to which manufacturers are subject before placing their products on the market. The Act follows a ‘risk-based’ approach, which means the higher the risk to cause harm to society, the stricter the rules. Furthermore, it establishes a legal framework for regulating high-risk AI systems, while those that do not meet the requirements to be considered as such will be regulated by codes of conduct. To this end, it classifies the risks that may result from AI uses as unacceptable risks or high, low or minimal risks.⁷²

Thus, it refers to AI systems as:

‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.⁷³

It also defines other important concepts related to AI, eg AI providers⁷⁴ or AI deployers,⁷⁵ and these definitions will serve as a reference for future legislative initiatives, such as the Proposal for AI Liability Directive.

As is the case for the European Parliament Resolution 2020, this Proposal includes a unilateral conflict rule, as it gives the Regulation an extraterritorial scope:

This Regulation applies to: (a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country; (b) deployers of AI systems that have their place of establishment or are located within the Union; (c) providers and deployers of AI systems that have their place of establishment or are located in a third country,

⁷² AI Act, art 5 and 6 et seq.

⁷³ AI Act, art 3(1).

⁷⁴ *ibid.* art 3(3) “‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge’.

⁷⁵ *ibid.* art 3 (4) “‘deployer’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity’.

where the output produced by the AI system is used in the Union.⁷⁶

This approach, which has already been used in other Regulations, eg in the General Data Protection Regulation (hereafter, GDPR),⁷⁷ may raise conflicting issues related to private international law, especially where service providers carry out their activity of providing services based on AI systems from a third state.

This is because, if the provider has foreseen that its services may be used in the EU market, the application of the Regulation will be justified; however, where a provider cannot be certain that its services will be used and may have an impact within the EU, the issue is more debatable, since the provider cannot control *ex ante* whether the AI system will be used by the user in that territory. In short, this issue is linked to the so-called International Stream of Commerce test and, where the provider has not directed the offer of its AI system services to users in the territory of the Union, the application of the Regulation to these providers will be more complex.⁷⁸

Therefore, having into account that AI systems incorporated in automated vehicles qualify as high-risk AI systems under the Regulation, it seems obvious that this legislation will apply to automated vehicles, hence the importance of this legislation when it enters into force.⁷⁹

3.3. The Proposal for a Directive on adapting non-contractual civil liability rules to AI

To complete the AI regulatory regime, the European Commission has recently launched two Proposals for a Directive directly related to the issue of AI and civil liability, the first of which is the Proposal for a Directive on adapting

⁷⁶ *ibid* art 2(1).

⁷⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L119/1, art 3(1), Territorial scope, states: 'This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.

⁷⁸ Pedro De Miguel Asensio considers that in these cases the application of the Regulation to these AI system providers is excessive if the use of their results in the Union is unforeseeable for him. 'Propuesta de Reglamento sobre inteligencia artificial', 92 *La Ley Unión Europea* (2021) 5.

⁷⁹ AI Act, art 6(1) (a) 'AI system shall be considered to be high-risk where both of the following conditions are fulfilled: the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I'.

non-contractual civil liability rules to AI (hereafter, AI Liability Act),⁸⁰ which harmonises certain national liability rules for AI and aims to facilitate fault-based tort claims, ie subjective liability and the recovery of compensation from victims of AI-related harm.

The Proposal complements the AI Act and, to ensure due consistency when referring to AI systems, AI providers and AI users, it invokes the definitions contained in that Act. In addition, the claims under the Directive are to be based on non-compliance with the specific obligations set out in the AI Act.

3.3.1 Objectives

This Directive aims to improve the functioning of the internal market by laying down uniform requirements for certain aspects of non-contractual civil liability for damage caused by the involvement of AI systems, and to adapt private law to the needs of the transition to the digital economy. In this way, it follows from the European Parliament Resolution 2020, which proposed to consider reversing the rules governing the burden of proof for harm caused by emerging digital technologies in clearly defined cases and put forward a strict liability regime for AI-enabled technologies. In some aspects, however, the Directive departs from the content of the Resolution

The question remains whether, with this Proposal, the Commission considers its legislative initiative in this area to be complete or, on the contrary, whether it remains open to the possibility of presenting other initiatives in the future in the field of broader civil liability, including contractual liability as well as non-contractual liability.

The latter option might be thought to be feasible, if we consider that the Proposal has chosen a development in two phases as the most appropriate policy option. In the first phase, it provides three measures to alleviate and facilitate the burden of proof for victims trying to prove their liability claim. In the second phase, it foresees the introduction of a review mechanism to re-assess, in particular, the need to harmonise strict liability for cases of AI use with a specific risk profile, as well as the possibility of including compulsory insurance⁸¹ – aspects that have already been included in the text of the European Parliament Resolution 2020.

The Directive then provides for a review five years after the end of the transposition period into national law. At that moment, the achievement of the

80 Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)', COM (2022) 496 final (Proposal for the AI Liability Directive).

81 AI Liability Directive, Explanatory memorandum, 9 where it says: 'the preferred policy option was developed and refined in light of feedback received from stakeholders throughout the impact assessment process to strike a balance between the needs expressed and concerns raised by all relevant stakeholder groups'.

objectives pursued will be examined, as well as the adequacy of no-fault liability rules for claims against the operators of certain AI systems insofar as they are not covered by other liability rules such as Directive 85/374/EEC. The need to establish compulsory insurance for the operation of specific AI systems will also be assessed, as suggested by European Parliament Resolution 2020.⁸²

3.3.2 *Scope of application*

The Directive applies to non-contractual civil law claims for damage caused by an AI system under fault-based liability regimes, that is to say, for a specific act or omission that has caused damage. It aims to simplify the procedures for the victim of a tort/delict to justify and prove it was the fault of a person or company that caused the damage. To this end, the Directive focuses on harmonising national rules on two specific aspects.

The first concerns the right of access by victims to relevant evidence from the defendant – a person subject to the obligations of a provider:⁸³ that is, access to information (disclosure of evidence) in relation to claims for damages based on non-contractual fault caused by high-risk AI systems. The aim is to facilitate the obtaining of compensation by victims in the case of subjective liability regimes that provide for liability to repair the damage caused intentionally or by a negligent act or omission.

The second aspect is that, with regard to the burden of proof before national courts in tort claims arising from damage caused by an AI system, the Proposal includes a presumption of a causal link between the defendant's fault and the damage caused by the AI system – the output produced by the AI system or the failure of the AI system to produce an output.⁸⁴ Nonetheless, the defendant shall have the right to rebut that presumption.

On the other hand, the Directive does not apply to criminal liability, nor will it affect the existing rules governing the conditions of liability in the transport sector, the rights that an injured person may have under national rules applicable by the transposition of Directive 85/374/EEC, or the exemptions from liability and due diligence obligations set out in the Digital Services Act.⁸⁵ Nor does it affect national provisions determining the party on whom the burden of proof rests, the standard of proof or the definition of fault,⁸⁶ except as provided for in arts 3 and 4, whereby the Directive complements the above-mentioned national provisions. In other words, the different national laws will continue to

⁸² *ibid* art 5.

⁸³ *ibid* art 1(1)(a).

⁸⁴ *ibid* art 1(1)(b).

⁸⁵ *ibid* art 1(2), final para and 1(3)(a), (b) and (c). See, Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC - COM (2020) 825 final.

⁸⁶ AI Liability Directive, art 1(3)(d).

apply on such relevant aspects as the strict liability regime or the reversal of the burden of proof.

3.3.3 *Victims' right of access to evidence and intervention by national courts*

a) Application by the injured party to their national courts

The Proposal for a Directive provides claimants of compensation caused by a high-risk AI system with the means of identifying the persons potentially liable for the harm and of excluding those who might appear to be falsely liable.⁸⁷ To this end, the Proposal foresees that potential claimants may go before national courts and request them to order providers, persons subject to the obligations of a provider or a deployer of an AI system⁸⁸ to disclose information available to them regarding the high-risk AI system suspected of having caused the harm. However, this must be a justified request. To ensure this, the Proposal adds that potential claimants must present sufficient facts and evidence to support such a claim and the admissibility of a claim for damages.⁸⁹ This implies that the supplier is required to retain this information as part of its obligations under the AI Act.⁹⁰

It is debatable whether, under certain circumstances, this obligation may be contradictory due to the high complexity that some AI systems may present, and because the party who has suffered the damage will not always have access to such facts or evidence. Consequently, these facts or evidence should be limited to the damage and negative effects suffered by the potential plaintiff. Otherwise, it will not be easy to prove this causal link if proof or evidence that are in the hands of the providers or users of the AI system, are lacking. It would be desirable, therefore, for courts to apply this provision flexibly; if they do not, it could lead to the refusal of the request for evidence from the potential tortfeasor.

In contrast, the court may only be asked to disclose evidence from providers and users of AI systems when the plaintiff has unsuccessfully tried to obtain such evidence directly from the defendant.⁹¹ However, if the persons mentioned above – the provider, the person subject to the provider's obligations or the user – refuse to comply with an order for disclosure of the evidence requested by the potential plaintiff, prior to their application to the court, this

⁸⁷ *ibid* Explanatory memorandum, 12.

⁸⁸ Pursuant to arts 16 et seq. of the AI Act.

⁸⁹ *ibid* art 3(1). The AI Act requires the providers to keep the documentation at the disposal of the national competent authorities for a period of ten years since the AI system has been introduced on the market or put into service. See art 50.

⁹⁰ AI Liability Directive, art 3 where it provides that 'national courts, upon the request of a claimant, are empowered to order specific measures to preserve the evidence mentioned in paragraph 1'.

⁹¹ *ibid* art 3(2).

should not justify the presumption of a breach of non-compliance with relevant duties of care on the part of these persons.⁹²

Furthermore, the request for disclosure of such evidence by the national courts shall be limited to that which is necessary and proportionate to substantiate the claim for damages.⁹³ This rule ensures proportionality in the disclosure of evidence and its limitation to the minimum amount required in order to prevent and avoid general requests.⁹⁴ In determining whether an order for disclosure or preservation of evidence is proportionate, national courts shall consider the legitimate interests of all parties, including interested third parties, in particular the protection of trade secrets and confidential information, e.g., relating to public or national security. They may also, at the request of the interested party, take necessary measures to protect the confidentiality of evidence used in legal proceedings.⁹⁵ These conditions make it possible to strike a balance between the rights of the complainant and the guarantees of the legitimate interests of other parties to the proceedings.

Finally, national courts must ensure that the person ordered to disclose or preserve the evidence mentioned above has access to appropriate procedural remedies in response to such orders.⁹⁶

b) Refusal of the requested party to comply with the national court's disclosure order

In the absence of compliance by the requested party with the order issued by a national court to disclose or preserve the evidence at its disposal by the conditions set out above, the national court shall presume that the defendant has not complied with a relevant duty of care respecting the evidence requested, which was intended to prove for the purposes of the claim for damages. Of course, this presumption may in any event be rebutted by the plaintiff.⁹⁷

3.3.4 Presumption of a causal link between fault and harm caused by AI systems

The Proposal for a Directive lays down a causality presumption in cases where a causal link between the harm and the activity carried out by the AI system can be considered reasonably likely from the circumstances in which the damage occurred.⁹⁸ However, as in the case of disclosure of evidence, the defendant shall have the option to rebut this presumption when they consider that the conditions giving rise to it are not met, in short, by proving that their

⁹² *ibid* recital n 17.

⁹³ *ibid* art 3(4).

⁹⁴ *ibid* Explanatory memorandum, 12.

⁹⁵ *ibid* art 3(4), second and third paras, and recital n 20.

⁹⁶ *ibid* art 3(4), fourth para.

⁹⁷ *ibid* art 3(1) and (5).

⁹⁸ *ibid* art 4(1).

fault could not have caused the damage.⁹⁹ In order to deal with the presumption of causal link, the Proposal distinguishes between high-risk AI systems, non-high-risk AI systems and the use of AI systems for non-professional activity.

a) Claims for damage caused by a high-risk AI system

In these cases, national courts shall consider the existence of a presumption of causation between the fault or omission of the defendant and the harmful result produced by the AI system, subject to the fulfilment of certain conditions.¹⁰⁰ At this point, it might be asked: when is the fault of the AI service provider or person subject to the provider's obligations considered to exist?

The Proposal for a Directive states that claims can be brought against a provider of a high-risk AI system, a person subject to the provider's obligations or a user of a high-risk AI system. The claimant must also prove the defendant's fault in accordance with the applicable EU or national rules.

So far as claims against the provider of a high-risk AI system or person subject to the provider's obligations under the AI Act are concerned, the defendant shall be deemed not to have complied with the duty of care laid down in Union law or national law where the claimant proves that they have failed to comply with any of the obligations laid down in Section 3, obligations of providers and deployers of high-risk AI systems and other parts, of the AI Act.¹⁰¹

By contrast, in the case of complaints against users of a high-risk AI system, those users shall be deemed not to have complied with the duty of care laid

⁹⁹ *ibid* art 4(7).

¹⁰⁰ *ibid* art 4(1). According to that provision, it will happen where all of the following conditions are met: (a) the claimant has demonstrated or the court has presumed pursuant to Article 3(5), the fault of the defendant, or of a person for whose behaviour the defendant is responsible, consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damage that occurred; (b) it can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output; (c) the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage'.

¹⁰¹ *ibid* art 4(2). According to that provision, these requirements are: '(a) the AI system is a system which makes use of techniques involving the training of models with data and which was not developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in [art 10(2) to (4) of the AI Act]; (b) the AI system was not designed and developed in a way that meets the transparency requirements laid down in [art 13 of the AI Act]; (c) the AI system was not designed and developed in a way that allows for an effective oversight by natural persons during the period in which the AI system is in use pursuant to [art 14 of the AI Act]; (d) the AI system was not designed and developed so as to achieve, in the light of its intended purpose, an appropriate level of accuracy, robustness and cybersecurity pursuant to [art 15 and art 16, point (a), of the AI Act]; or (e) the necessary corrective actions were not immediately taken to bring the AI system in conformity with the obligations laid down in [Title III, Chapter 2 of the AI Act] or to withdraw or recall the system, as appropriate, pursuant to [art 16, point (g), and art 21 of the AI Act]'.

down in Union or national law where the complainant proves that the user¹⁰² has failed to comply with their obligations to use and monitor the AI system in accordance with the instructions for use that accompanied it or; where applicable, failed to suspend or discontinue its use according to the AI Act;¹⁰³ or exposed the AI system to input data under its control that is not relevant in view of the system's intended purpose pursuant to the AI Act.¹⁰⁴

In addition, where the defendant demonstrates the existence of sufficient and reasonably accessible evidence for the claimant to prove the causal link between the defendant's fault or omission and the harmful result produced by the AI system, the national court will not apply the causal link presumption.¹⁰⁵ This is an exception to the causation principle; it is up to the defendant who has breached the rules to prove that this breach has not caused harm because there are other explanations for it.

b) Claims for damage caused by non-high-risk AI systems

Respecting claims for damage caused by non-high-risk AI systems, the presumption of causation shall only apply if the national court considers it excessively difficult for the claimant to prove the causal link between the fault and the output produced by the AI system, or the failure of the AI system to produce an output.¹⁰⁶

c) Claims for damage caused by AI systems used in the course of a personal, non-professional activity

Where the AI system was used for personal, non-professional use, the presumption of causation will apply only where the defendant has materially interfered with the operating conditions of the AI system, or if they might have been required to (and could have) determined the operating conditions of the AI system, but failed to do so.¹⁰⁷ This distinction seeks to strike a balance between the interests of injured persons' and non-professional users' by not applying the presumption of causation when non-professional users do not add risks through their behaviour.¹⁰⁸

102 *ibid* art 4(3)

103 *ibid* art 4(3)(a). See AI Act, art 26.

104 *ibid* art 4(3)(b). See AI Act, art 26.

105 *ibid* art 4(4).

106 *ibid* art 4(5).

107 *ibid* art 4(6).

108 *ibid* Explanatory memorandum, 14.

3.4. The Proposal for a Directive liability for defective products

3.4.1 Objectives

Alongside the AI Liability Directive, the European Commission has also presented a Proposal for a Directive on liability for defective products (hereafter, Product Liability Directive).¹⁰⁹ This Proposal aims to provide an EU legal framework for compensating people who suffer physical injury or damage to property due to defective products. It adapts the text of Directive 85/374/EEC (which has been applied in the European Union for more than 35 years) to the digital age and that Directive will therefore be repealed when the new one enters into force. In order to fulfil its aims, the Proposal lays down ‘common rules on the liability of economic operators for damage suffered by natural persons caused by defective products’¹¹⁰ and provides for uniform harmonisation of civil liability law in Member States. To ensure a similar level of protection in all Member States, it does not allow for the adoption of more or less stringent standards.¹¹¹

Similar to the AI liability Directive, the Proposal for a Product Liability Directive seeks to alleviate the burden of proof of the claimant in complex cases, for instance involving AI systems, and also when it came to products that fail to comply with safety requirements.¹¹²

Thus, the Proposal is consistent with existing instruments concerning liability and, at the same time, complements the Proposal for an AI Liability Directive, so there is no overlap with claims that may be brought under both Directives.¹¹³

In the light of this Proposal, it is obvious that businesses must improve the safety of their products and services linked to digital technologies, including those related to AI; otherwise, they may cause damage and, in such cases, the right of injured parties to obtain compensation must be guaranteed.

3.4.2 AI systems and the notion of ‘product’

Among the most relevant aspects introduced by the Proposal is that AI systems and AI-enabled goods are considered as ‘products’. This means that they fall within the scope of the Product Liability Directive, and the damage caused by defective AI systems may be the subject of a claim by the injured person

109 Commission ‘Proposal for a Directive of the European Parliament and of the Council on liability for defective products’ COM (2022) 495 final.

110 Directive for Defective Products, art 1.

111 *ibid* art 3.

112 In order to ensure the adaptation of liability rules to AI, these provisions of the Proposal for a Directive follow to a large extent the provisions included in the European Parliament Resolution 2020, and the Proposal for a Regulation included therein. Explanatory memorandum, para 1.3.

113 Directive for Defective Products, Explanatory memorandum, paras 1.2 and 1.3.

without it being necessary to prove the tortfeasor's fault.¹¹⁴ Therefore, in order to adapt the content of the current Directive on defective products to the reality of products in the digital age – which can be tangible or intangible – the Proposal includes 'digital manufacturing files and software' within the definition of 'product'.¹¹⁵ It also defines when a related service is to be treated as a component of a product.¹¹⁶

3.4.3 Defectiveness of a product and the right to compensation

As far as the product's defectiveness is concerned, the Proposal refers to products that do not provide the safety that a user is entitled to expect, including safety-relevant cybersecurity requirements.¹¹⁷ To determine defectiveness, an objective analysis should be carried out, taking into account the intended purpose and the objective characteristics and properties of the product, as well as the expectations and requirements of the users for whom the product is intended.¹¹⁸

Nonetheless, there is an exclusion and a product shall not be considered to be defective 'for the sole reason that a better product, including updates or upgrades to a product, is already or subsequently placed on the market or put into service'.¹¹⁹

The Member States shall also ensure the right of any natural person who suffers damage (material losses) caused by a defective product to obtain adequate (full and proper) compensation. Furthermore, this right shall extend to persons subrogate to the right of the injured person or acting on behalf thereof,¹²⁰ even

¹¹⁴ *ibid* Explanatory memorandum, para 1.3.

¹¹⁵ *ibid* art 4(1) and (2) which defines "digital manufacturing file" as a digital version or a digital template of a movable'. As referred to in recital n 12 of the Directive 'Software, such as operating systems, firmware, computer programs, applications or AI systems, is increasingly common on the market and plays an increasingly important role for product safety'; and in recital n 14 'Digital manufacturing files, which contain the functional information necessary to produce a tangible item by enabling the automated control of machinery or tools, such as drills, lathes, mills and 3D printers, should be considered as products, in order to ensure consumer protection in cases where such files are defective'.

¹¹⁶ According to Directive for Defective Products "component" means any item, whether tangible or intangible, or any related service, that is integrated into, or inter-connected with, a product by the manufacturer of that product or within that manufacturer's control; meanwhile "related service" means a digital service that is integrated into, or inter-connected with, a product in such a way that its absence would prevent the product from performing one or more of its functions'. See arts 4(3) and (4) respectively.

¹¹⁷ *ibid* art 6(1)(f).

¹¹⁸ *ibid* recital n 22.

¹¹⁹ *ibid* art 6(2).

¹²⁰ *ibid* art 5.

though rules on calculating compensation should be laid down by Member States.¹²¹

3.4.4 *Liability for defective products*

Concerning the persons who may be held liable for damage, the Proposal includes hardware manufacturers, software providers and providers of digital services that affect how the product works, eg (in the field of autonomous driving) the navigation software development service that is installed in these vehicles. Moreover, the Proposal ensures that manufacturers can be held liable for changes they make to products already on the market, even if those changes are due to software updates or machine learning.¹²²

Regarding product liability, the Proposal distinguishes between the type of operator involved in each case. First, it determines when the manufacturer of the defective product shall be liable. In this regard, it considers that any natural or legal person who modifies a product that has already been placed on the market or put into service in the course of a commercial activity shall be regarded as a manufacturer. However, such a modification must be considered substantial under the relevant Union or national product safety rules and carried out outside the control of the original manufacturer. Likewise, the manufacturer of a defective component that has caused the product to be defective will be held liable.¹²³

Second, the Proposal regulates the liability of manufacturers established outside the EU. In these cases, the following distinction must be made. If the importer of the defective product and the manufacturer's authorised representative are established in the territory of the Union, they can be held liable for damage caused by the defective product. However, if neither of them is established in the EU, the fulfilment service provider may be held responsible for the damage.¹²⁴

Third, where the above-mentioned operators – manufacturer, importer, authorised representative of the manufacturer or fulfilment service provider – cannot be identified, the Proposal states that Member States shall ensure that each distributor of the product can be held liable provided that certain conditions are met.¹²⁵

121 According to recital n 18 of the Proposal, material losses includes those 'resulting from death, or personal injury, or damage to or destruction of property and data loss or corruption'. But the Directive should not affect national rules relating to non-material damage.

122 *ibid* Explanatory memorandum, para 1.3.

123 *ibid* arts 7(1) and 7(4).

124 *ibid* arts 7(2) and 7(3).

125 *ibid* art 7(5), where the following conditions are set out: '(a) the claimant requests that distributor to identify the economic operator or the person who supplied the distributor with the product; and (b) the distributor fails to identify the economic operator or the person who supplied the distributor with the product within 1 month of receiving the request'.

Fourth, the Proposal also refers to online contracting and sets up the responsibility of providers of an online platform that is not a manufacturer, importer or distributor and which enables consumers to conclude distance contracts with traders, provided that the conditions of the Digital Services Act are met.¹²⁶

Fifth and finally, it provides for the joint and several liability of those (multiple) economic operators which, in accordance with the provisions of the Directive, may be held liable for the same damage.¹²⁷

3.4.5 Proceedings for claiming

a) Disclosure of evidence

In order to claim compensation from the operator responsible for the defective product that caused the damage, injured parties who have presented facts and evidence to support the plausibility of such a claim may request and obtain relevant evidence. In this respect, the Proposal provides that Member States should ensure that national courts have the power to order the defendant to disclose the relevant evidence at its disposal.¹²⁸

However, Member States should ensure that national courts limit the disclosure of evidence to what is necessary and proportionate. In doing so, they shall take into account the legitimate interests of all parties, including the third parties concerned, in particular in relation to the protection of confidential information and business secrets within the meaning of art 2(1) of Directive (EU) 2016/943.¹²⁹ Member States shall also take specific measures necessary to preserve the confidentiality of such information when it is used or referred to in the course of judicial proceedings.¹³⁰

b) Limitation periods to initiate proceedings for claiming

The Proposal sets up different limitation periods. First of all, there will be a limitation period of three years applicable to initiating proceedings for claiming compensation for damage caused by defective products according to the

¹²⁶ *ibid* art 7(6).

¹²⁷ *ibid* art 11.

¹²⁸ *ibid* art 8(1).

¹²⁹ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure[2016] OJ L157/1, art 2(1) sets up: “‘trade secret’ means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret’.

¹³⁰ Directive for Defective Products, art 8 paras 2-4.

Directive. However, issues relating to the suspension and interruption of limitation periods will continue to be governed by national law.

To determine the start of this three-year period, the Proposal provides that it will run from the day on which the injured person became aware, or should reasonably have become aware, of all of the following: the damage; the defectiveness of the product; and the identity of the economic operator that can be held liable.¹³¹ According to the Proposal's wording, it should therefore be understood that these elements must be fulfilled cumulatively, and that the time limit will not start to run until the injured party has become aware of all three. The problem will arise in cases where it is possible to identify the damage and the tortfeasor, but not the defect that has caused it when, for example, AI systems are involved.

Second, the Directive provides for the extinction of the rights conferred on the injured person under the Directive after the expiry of a limitation period of 10 years. This period will begin to run from the date on which the defective product which caused the damage was placed on the market, put into service or substantially modified, unless in the meantime the claimant has initiated proceedings before a national court against the economic operator who may be held liable.¹³² This limitation period may exceptionally be extended up to 15 years when the injured person has not been able to initiate proceedings within 10 years due to the latency of a personal injury.¹³³

3.4.6 *Burden of proof*

As a general principle, the Proposal for a Directive sets up the obligation of the claimant to prove the defectiveness of the product, the damage suffered and the causal link between the defectiveness and the damage, that is to say, the burden of proof is on the injured person.¹³⁴ In this sense, to ease this burden, the defectiveness of the product shall be presumed where some conditions are met, eg non-compliance with mandatory safety requirements or the obvious malfunction of the product.¹³⁵

It will be presumed that there is a causal link between the defectiveness of the product and the damage, where it has been found that the product is

¹³¹ *ibid* art 14(1).

¹³² *ibid* art 14(2).

¹³³ *ibid* art 14(3).

¹³⁴ *ibid* art 9(1).

¹³⁵ *ibid* art 9(2) According to that provision, any of the following conditions should met: '(a) the defendant has failed to comply with an obligation to disclose relevant evidence at its disposal pursuant to Article 8(1); (b) the claimant establishes that the product does not comply with mandatory safety requirements laid down in Union law or national law that are intended to protect against the risk of the damage that has occurred; or (c) the claimant establishes that the damage was caused by an obvious malfunction of the product during normal use or under ordinary circumstances'.

defective and the damage caused is of a kind typically consistent with the defect in question.¹³⁶

It is now necessary to examine what will happen if the claimant cannot prove the defectiveness of the product or the causal link between the defectiveness and the damage caused. In such cases, where national courts consider that the claimant faces excessive difficulties for the burden of proof due to technical or scientific issues, there will be a presumption of defectiveness and a causal link where the claimant has demonstrated that: '(a) the product contributed to the damage, and (b) it is likely that the product was defective or that its defectiveness is a likely cause of the damage, or both'.¹³⁷

In any event, the Proposal provides that the defendant shall have the right to contest the existence of excessive difficulties in proving the defectiveness of the product or the causal link between defect and damage, as well as the right to rebut any of the presumptions set out above.¹³⁸

3.4.7 Exemption, reduction, exclusion or limitation of liability

Economic operators – manufacturers, importers or distributors – might be excluded from liability for damage caused by defective products, provided they can prove the existence of any of the circumstances foreseen in the Proposal.¹³⁹ Nevertheless, where the defectiveness that caused the damage did not exist when the product was placed on the market, put into service or (respecting a distributor) made available on the market, or where this defectiveness came into being after that moment, the economic operator's exemption from liability shall not apply where the defectiveness of the product is due to a related service; to software, including software updates; or to failure to update the software as

¹³⁶ *ibid* art 9(3).

¹³⁷ *ibid* art 9(4) last para.

¹³⁸ *ibid* art 9(4) and 9(5).

¹³⁹ *ibid* art 10(1) which sets the following circumstances: '(a) in the case of a manufacturer or importer, that it did not place the product on the market or put it into service; (b) in the case of a distributor, that it did not make the product available on the market; (c) that it is probable that the defectiveness that caused the damage did not exist when the product was placed on the market, put into service or, in respect of a distributor, made available on the market, or that this defectiveness came into being after that moment; (d) that the defectiveness is due to compliance of the product with mandatory regulations issued by public authorities; (e) in the case of a manufacturer, that the objective state of scientific and technical knowledge at the time when the product was placed on the market, put into service or in the period in which the product was within the manufacturer's control was not such that the defectiveness could be discovered; (f) in the case of a manufacturer of a defective component referred to in Article 7(1), second subparagraph, that the defectiveness of the product is attributable to the design of the product in which the component has been integrated or to the instructions given by the manufacturer of that product to the manufacturer of the component; or (g) in the case of a person that modifies a product as referred to in Article 7(4), that the defectiveness that caused the damage is related to a part of the product not affected by the modification'.

necessary to ensure its security, provided that this is within the manufacturer's control.¹⁴⁰

The Proposal provides for the reduction of liability when the damage is caused by both the defectiveness of the product and the fault of the injured party, or of a third party for whom the injured party is responsible.¹⁴¹ However, this compels Member States not to reduce the liability of economic operators when the damage is caused by both the defectiveness of the product and by an act or omission of a third party, without distinguishing whether that third party has any connection with the operator.¹⁴²

Lastly, the Proposal obliges Member States to ensure that the liability of an economic operator under this Directive is not limited or excluded, in relation to the injured party, by a contractual provision or by national law.¹⁴³

4. Compatibility of the AI liability regime with the rules of private international law

4.1. Territorial scope of the Commission Proposals for a Regulation

Neither the Proposal for a Regulation included in the European Parliament Resolution 2020, nor the Proposal for a Regulation (AI Act), expressly refers to the introduction of private international law rules. As illustrated, both Proposals include unilateral conflict rules characterised by their extraterritorial scope, which may have an impact on the system of private international law currently in force. In this context, it is now necessary to examine some relevant questions.

The first relates to the interpretative doubts raised by art 2(1) of the Proposal for a Regulation included in the European Parliament Resolution 2020. Thus, when referring to damage caused in the territory of the Union, is it considered that the person affected must also be permanently present in that territory, ie habitually resident there? In contrast, would a temporary presence in that territory be sufficient if the person were in the territory of the Union on holiday or on a business trip?

Since the Proposal does not distinguish between these situations, the AI Act¹⁴⁴ – which also establishes a unilateral conflict rule with regard to its scope

¹⁴⁰ *ibid* art 10(2) in connection with provisions of 10(c).

¹⁴¹ *ibid* art 12(2).

¹⁴² *ibid* art 12(1).

¹⁴³ *ibid* art 13.

¹⁴⁴ AI Act, art. 2(1) states: '1. This Regulation applies to: (a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country; (b) deployers of AI systems that have their place of establishment or are

– could apply by analogy in order to clarify this question. Accordingly, one must admit that it will suffice that the user of AI systems should be in the territory of the Union at the time of the damage; or even that the user should be in a third country, provided that the consequences of the use of AI systems occur within the territory of the Union, eg because the user of the AI systems provides services to companies located in the European Union.

On the other hand, in order to assess whether the AI system that caused the damage was developed in the territory of the European Union, would it be sufficient for the result of the damage to occur in the European Union, or is it also necessary that the system should be established in that territory?¹⁴⁵ Again, the extensive interpretation of art 2(1) of the AI Act may be helpful in answering this question. The Act states that providers may be established in the EU or in a third country. More particularly with regard to AI systems, it states that the information generated by the system must be used in the EU. Consequently, the damage must occur in the territory of the Union, irrespective of where the operator is located.

In addition, it should be borne in mind that, in some cases, damage may materialise virtually, ergo, that the principle of *lex loci damni* may be burdensome for certain companies when they are established outside the European Union and cannot foresee that damage may occur within the territory of the Union. In such case, this rule could be considered exorbitant.

All this being said, it should not be forgotten that the unilateral conflict rule seeks to protect the interests of citizens within the European Union. However, the internal market of the EU is of great interest to companies operating in the field of AI, which may compensate for the fact that they are subject to EU rules in such a matter.

The second question relating to territorial scope of the Commission Proposals for a Regulation, would be what will happen in cases where the AI system causes damage outside the Union? In principle, the application of the referred Regulations should be excluded, according to their current wording.¹⁴⁶ In such cases, it seems reasonable to resort to the general system of sources of

located within the Union; (c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union; (d) importers and distributors of AI systems; (e) product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark; (f) authorised representatives of providers, which are not established in the Union; (g) affected persons that are located in the Union’.

145 Alexia Pato, ‘The EU’s upcoming regulatory framework on Artificial Intelligence and its impact on PIL’ (EAPIL, 12 July 2021) <<https://capil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/>> accessed 31 March 2023.

146 European Parliament Resolution 2020, art 2 Text of the Proposal for a Regulation requested, and AI Act, art 2.

private international law to determine the law applicable to the non-contractual liability arising from the damage caused by AI systems.

The third question arises with respect to the condition established in the Proposal for a Regulation included in the European Parliament Resolution 2020. It will apply

Where a physical or virtual activity, device or process driven by an AI-system has caused harm or damage to the life, health, physical integrity of a natural person, to the property of a natural or legal person or has caused significant immaterial harm resulting in a verifiable economic loss.¹⁴⁷

This wording also raises interpretative difficulties regarding the delimitation of the concept of ‘significant’ and, in the absence of an autonomous and uniform definition or interpretation, we will have to refer to national rules and case law.

The fourth and final question, concerns the possibility of applying a foreign law. Taking into account the unilateral nature of these rules, neither the AI Act nor the Proposal for a Regulation included in the European Parliament Resolution 2020 responds to this question. It is therefore not clear when a foreign law may be applicable in cases of non-contractual liability arising from the use of AI systems; nor do these texts suggest the possibility of incorporating a specific conflict rule in other existing instruments for claims arising out of the use of AI. It would, therefore, be necessary to resort to the rules of private international law that are generally applicable in this area, whether the Rome II Regulation or The Hague Conventions of 1971 or 1973.

4.2. Interaction with the Brussels I-bis Regulation, the Rome II Regulation and the Hague Conventions

Where the damage occurs in the territory of the Union, the two rules included in the scope of the above-mentioned Proposals for a Regulation establish a direct link with one of the 27 Member States and, consequently, with their courts, which may have jurisdiction based on the place where the harmful event occurred.¹⁴⁸ The question will be whether these rules prevail over the application of the provisions laid down in the Brussels I-bis Regulation.¹⁴⁹ In principle, it should be noted that these rules are not incompatible, as they are delimiting the

¹⁴⁷ *ibid* art 2(1) and recital n 16. AI Act, recital n 4 also refers to immaterial harm when states that: ‘depending on the circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial’.

¹⁴⁸ Brussels I-bis Regulation, art 7(2).

¹⁴⁹ *ibid* art 67, which provides: ‘This Regulation shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union or in national legislation harmonised

place where the damage occurred within the territory of the European Union; nor do they prevent the application of the rule of general jurisdiction (the forum of the defendant's domicile) provided for in the Brussels I-bis Regulation where the injured party wishes to sue before that court.¹⁵⁰

As far as the applicable law is concerned, the mentioned unilateral conflict rules will prevail over the Rome II Regulation, as they are provisions of Community law applicable to liability arising out of non-contractual obligations.¹⁵¹ In this context, it seems necessary to examine the interplay of these rules with conflict rules provided in other international instruments of private international law.

Furthermore, the Proposal for a Regulation included in the European Parliament Resolution 2020 limits party autonomy by considering any agreement to be void between an operator of an AI system and an injured party – natural or legal person – which circumvents or limits the rights and obligations set out in the Regulation.¹⁵² In short, the Regulation would allow the parties to choose the applicable law as long as this respects the rights and obligations contained in the Regulation. In a way, this provision has some parallels with the party autonomy principle foreseen in the Rome II Regulation, which allows the parties to agree to submit non-contractual obligations to the law of their choice, albeit with certain limits.¹⁵³

It is now necessary to refer to liability arising from defective products and cross-border traffic accidents, since both situations are subject to special conflict rules.

As far as defective products are concerned, the Rome II Regulation provides for the habitual residence of the injured party as the connecting factor, which is given preference over the *lex loci damni* conflict rule foreseen in both Proposals for a Regulation mentioned above.¹⁵⁴ This is despite the fact that, in such cases, the 1973 Hague Convention on the Law Applicable to Product Liability is to be applied in preference to the Rome II Regulation by the courts of Member States which are contracting parties to this Convention. As is the case with the

pursuant to such instruments'. See Benedetta Cappiello, *AI-systems and non-contractual liability. A european private international law analysis* (Giappichelli Editore 2022) 36.

150 *ibid* art 4.

151 Rome II Regulation, art 27 states: 'This Regulation shall not prejudice the application of provisions of Community law which, in relation to particular matters, lay down conflict-of-law rules relating to non-contractual obligations'.

152 European Parliament Resolution 2020, art 2(2): 'Any agreement between an operator of an AI-system and a natural or legal person who suffers harm or damage because of the AI-system, which circumvents or limits the rights and obligations set out in this Regulation, concluded before or after the harm or damage occurred, shall be deemed null and void as regards the rights and obligations laid down in this Regulation'.

153 Rome II Regulation, art. 14(2) and (3) in relation to art. 16 (overriding mandatory provisions) and art 26 (public policy of the forum).

154 *ibid* art 5.

Rome II Regulation, the Convention also lays down conflict rules where the connecting factor of the habitual residence of the injured party prevails over the *lex loci damni* criterion.¹⁵⁵

In matters relating to liability arising from cross-border traffic accidents, the Rome II Regulation does not provide for a specific rule and, therefore, the general rule will apply.¹⁵⁶ However, the 1971 Hague Convention on the Law Applicable to Road Traffic Accidents prevails over the general rule of the Rome II Regulation and, although the Convention establishes the *lex loci delicti* as the general criterion, it is important to note that this principle is subject to certain exceptions.¹⁵⁷

Finally, given that neither the 1971 nor the 1973 Hague Conventions incorporate party autonomy, the parties may resort to the Rome II Regulation, which foresees such an option 'by an agreement entered into after the event giving rise to the damage occurred; or where all the parties are pursuing a commercial activity, also by an agreement freely negotiated before the event giving rise to the damage occurred'.¹⁵⁸

In this context, should the Proposals for a Regulation be adopted as currently drafted, the main consequence will be that the unilateral conflict rules included therein may create problems in the area of tort liability arising from the use of AI systems in automated driving. On the one hand, this is because the existing instruments will remain applicable to cases where the damage caused by an AI system does not occur within the territory of the European Union; on the other hand, it is because, where the damage occurs within the territory of the Union, the aforementioned unilateral conflict rules will make the predictability of applicable law more complex due to the coexistence of different regulatory instruments of application in this area.

5. Conclusion

The recent package of legislative measures launched by the European Commission in the field of AI and non-contractual civil liability constitutes a legal framework adapted to the robotisation and automation of our society, and makes it possible to harmonise national legislation in these matters. These Proposals allow us to reflect on the need to reform and harmonise the regulatory framework in force, particularly in the field of private international law, and especially to ensure its adaptation to aspects related to AI and automated

¹⁵⁵ 1973 Hague Convention, arts 4-7.

¹⁵⁶ Rome II Regulation, art 4.

¹⁵⁷ 1971 Hague Convention, arts 4-6.

¹⁵⁸ Rome II Regulation, art 14.

driving, and to provide an adequate response to the challenges and risks that may arise in future in this sector.

As explained earlier, the unilateral conflict rules included in the Proposals for a Regulation limits party autonomy and states the *lex loci damni* as the only connecting point. In consequence, they do not foresee other connections that may be more favourable to the injured party, such as habitual residence or the more closely connected principle. This circumstance will be particularly important in claims arising from automated driving and damages suffered in the territory of the European Union by persons who do not have their habitual residence in one Member State, since extraterritoriality of the Community rules will apply and the parties will not be able to choose the applicable law.

Moreover, it is debatable whether the *lex loci damni* rule would be appropriate for cases of damage caused through the internet, where the physical location of the damage is complex or where different places may concur.¹⁵⁹ Bearing in mind that the damage could occur in any country of the European Union, this would also be relevant, considering the lack of harmonisation of Member States' legislation in terms of such relevant aspects as, for example, those relating to the scope of compensation and limitation periods.

Furthermore, the unilateral conflict rule foreseen in the Proposal for a Regulation included in the European Parliament Resolution 2020 would only affect the 'operator' – initial and/or final – of an AI system. This means that claims against producers of defective AI systems, or against third parties who interfere by using the AI system to cause harm (as long as they have no control over the AI systems), will continue to be governed by the system envisaged in the Rome II Regulation and the 1973 Hague Convention.

Finally, both Proposals consider that AI may cause material or immaterial harms, and, when referring to immaterial harm, they require that it has to be significant immaterial harm resulting in a verifiable economic loss. Otherwise, it must be understood that the immaterial harm falls outside its application and, accordingly, the civil liability derived from these damages will also be subject to the Rome II Regulation.

In turn, the two recent Proposals for a Directive (on AI liability and liability for defective products) are both to be welcomed, since they present positive and innovative aspects for adapting non-contractual civil liability rules to AI, particularly the liability arising from using defective products based on AI systems. It is obvious that both norms will allow for a proper coordination and harmonisation of the civil liability regimes applicable to AI systems in the EU, eliminating the risk of fragmentation of national rules in this matter and the consequent negative effect of this on the proper functioning of the internal

159 Eva Lein, *Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations* (British Institute of International and Comparative Law 2021), 73.

market. At the same time, they will ensure the unification of the applicable law irrespective of the law designated by the conflict rule, where the law of a Member State is involved.

In this way, the risk-based regulatory approach aimed at ensuring that high-risk AI systems comply with safety and fundamental rights requirements can be considered appropriate, also allowing for the alleged infringer to rebut the presumption of defectiveness of the product. Hence, such an approach would ensure a fair balance between manufacturers and consumers and contribute to creating a safe and reliable environment for developing AI systems within the European Union.

Another important question is whether the provisions contained in the two Proposals for a Directive could be considered as overriding mandatory provisions. If yes, the main consequence will be that they will be applicable by the courts of the EU Member States, irrespective of the law designated by the conflict rule.

To conclude, one must admit that the private international law provisions currently in force should be sufficient to provide an adequate answer to the questions of non-contractual liability arising from the use of AI systems in automated vehicles. Nevertheless, better coordination of these instruments will be necessary, either by considering the denunciation of the Hague Conventions of 1971 and 1973 or by introducing some modifications to the Rome II Regulation to bring it into line with the Conventions. In the absence of this, it would be desirable for new legislative initiatives, such as those analysed in this paper, to include conflict rules that follow the same criteria established by the above-mentioned instruments, in order to avoid this legislative dispersion making the already complex application of these rules more difficult.

Blockchain As a New Vehicle of Electronic Evidence in China

Yong Zhang *

Faculty of Law, University of Macau
ORCID 0009-0002-0748-5779

Qianyi Yan **

Faculty of Law, University of Macau
ORCID 0009-0008-3740-2106

DOI: 10.54103/milanoup.215.c449

Abstract

The rapid development of blockchain technology has prompted its application to e-commerce anti-counterfeiting, personal identity authentication, transparency of transaction information, and other aspects. Meanwhile, social communication has gradually tended to be dominated by electronic data. Against this background, electronic evidence storage on blockchain came into being. This paper, firstly, through a literature review, will address the extension of the concept of digital evidence in the new era of blockchain, relevant legal provisions of China on the legal effect of electronic evidence stored in the blockchain, as well as the significance of the application of blockchain in generating digital evidence in the Chinese legal system. Secondly, through case analysis, it will analyze the first case decided in China based on digital evidence preserved by blockchain technology. Including the storage, collection, and verification procedures of electronic evidence in the blockchain, as well as technical and legal issues of applying electronic evidence stored in the blockchain. Such as the technical risk of the password being cracked, the legal problem that the authenticity of the evidence is difficult to determine, and so on. Thirdly, through a comparative law perspective, it will analyze how the USA treats electronic evidence stored in the blockchain, the ways that they solve the above problems, and whether it can achieve cross-border blockchain electronic evidence

* Yong Zhang, Ph.D. Candidate, University Teaching Assistant, Faculty of Law, University of Macau, Macau Special Administrative Region, China. Research fields: Technology Law, Digital Law.

** Qianyi Yan, Lecturer, Xianda College of Economics and Humanities, Shanghai International Studies University, Shanghai, China. Research fields: Artificial Intelligence, Blockchain.

assistance. Fourthly, it will be discussed the possibility that in the coming future, while increasing the credibility of the digital evidence generation system and strengthening the evidence preservation process, the generality of judicial entities could recognize the legal status of digital evidence preserved by blockchain technology.

Keywords

Electronic Evidence; Arbitration Chain; Blockchain Evidence; The USA; Authenticity of Blockchain Evidence

1. Introduction

With the rapid popularization of the Internet, the volume of online transactions is increasing day by day. Among them, online transactions in banking, securities, insurance, e-commerce, and other fields are very significant. For example, in 2017, the scale of e-commerce transactions in China was 28.66 trillion yuan, up 24.77% year on year. Among them, the B2B turnover was 20.5 trillion yuan, the online retail turnover was 7.17 trillion yuan, and the domestic service e-commerce turnover was 998.6 billion yuan.¹ Online transactions have become an increasingly important part of people's lives, and even overtaken cash transactions and physical store transactions. Electronic bills are inevitable during the process. The transaction volume of online transfers is huge, and real-time statistics of platform transaction volume have become a problem that financial institutions need to solve at present. Many financial institutions currently conduct online statistics to ensure the authenticity of their data as much as possible. Considering the characteristics of electronic data such as virtuality and falsifiability, once online disputes occur, it becomes a problem whether these data can be recognized by judicial institutions.²

On the other hand, because electronic evidence involves strong professional skills and most judicial personnel lack high-tech knowledge, they are limited by professional knowledge in the process of adopting electronic evidence. At present, although there are relevant laws and regulations on the identification of electronic evidence, there has not yet been any organization that is engaged in such business for society, which will bring about difficulties in the identification of electronic evidence in litigation. Given the system dependence and high technology of electronic evidence, the collection process of electronic evidence is highly demanding for technology. It is difficult even for those who

1 E-commerce Research Center, '2017 China E-commerce Market Data Monitoring Report' (*China Economic Net*, 1 June 2018) <www.100ec.cn/zt/17market_data_report/> accessed 15 April 2023.

2 Ethel, 'Blockchain Joins Arbitration Industry First Arbitration Chain Appears in Shenzhen' (*Chaintiao*, 1 May 2020).

have been engaged in judicial work for a long time to extract electronic evidence professionally.³

2. Literature review

2.1 Characteristics, legal provisions, and evidence collection methods of e-evidence

Electronic evidence has appeared and has been applied in judicial practice in China for more than 20 years. Its legal status was formally established in the Criminal Procedure Law⁴ and Civil Procedure Law⁵, which came into effect in 2013. The prototype of electronic evidence has been reflected in the Contract Law 1999⁶ and the Electronic Signature Law 2004⁷. E-mail, electronic data exchange, online chat records, online blogs, mobile phone SMS, electronic signatures, domain names, etc. were defined as the form of electronic evidence for the first time in the Provisions on Several Issues Concerning Examination and Judgment of Evidence in Death Penalty Cases jointly issued by the Supreme People's Court, the Supreme People's Procuratorate and other departments in 2010.⁸ In the field of civil procedure law, electronic data has officially appeared as an independent type of evidence in the Civil Procedure Law revised in 2012.⁹ The judicial interpretation of the Civil Procedure Law issued in 2015 defines in detail electronic data as the type of civil evidence and clearly distinguishes between electronic data and audio-visual materials. It also clearly points out that electronic data refers to information formed or stored in electronic media through e-mail, electronic data exchange, online chat records, blogs, microblogs, mobile phone SMS, electronic signatures, domain names, etc.¹⁰

Regarding the characteristics of electronic evidence, Du Chunpeng put forward the intangibility and vulnerability of electronic evidence.¹¹ Electronic evidence is intangible in that it exists in the media in the form of sound, light, electricity, magnetism, etc. and is an electromagnetic wave and binary data coding in

3 Liu Huijie, 'Collection Measures, Methods and Precautions of Electronic Evidence' (*Baidu Wenku*, 2 November 2012) <<https://wenku.baidu.com/view/6e63e1156edb6f1aff001f5d.html?re=view>> accessed 15 April 2023.

4 Criminal Procedure Law of the People's Republic of China 2013, art 48.

5 Civil Procedure Law of the People's Republic of China 2013.

6 Contract Law of the People's Republic of China 1999, art 11.

7 Electronic Signature Law of the People's Republic of China 2004, art 2.

8 Provisions on Several Issues Concerning Examination and Judgment of Evidence in Death Penalty Cases 2010, art 29.

9 Civil Procedure Law of the People's Republic of China 2013, art 63.

10 Judicial Interpretation of the Civil Procedure Law 2015, art 116.

11 Chunpeng Du, *Collection and Identification of Electronic Evidence* (China University of Political Science and Law Press 2014).

nature, so it is difficult to collect. Because of its intangibility, its security and authenticity are easily damaged by the outside world, and even sometimes the facts it reflects are not the essential truth, but only the apparent truth. Examples are filmed images of disguised persons or objects, audio recordings imitated, link titles inconsistent with link web addresses and contents, virtual screen names inconsistent with real identities, web pages tampered with by ‘hackers’, forged e-mails, etc. If these evidences are not corroborated by third-party evidence, there is a high possibility that they will be misjudged. Regarding the vulnerability of electronic evidence, whether in digital or analog form, it is extremely vulnerable to external damages, such as monitoring, eavesdropping, interception, tampering, and deletion during its storage, transmission, and use, because it is stored on erasable data recording media, such as magnetic tape, magnetic disk, erasable optical disk, and is easily damaged due to misoperation in use. In addition, Zhou Lingling also proposed the technical and composite characteristics of electronic evidence.¹² The technical characteristic of electronic evidence refers to that electronic evidence depends on certain technical equipment and means. In addition, the electronic evidence integrates text, images, pictures, sounds, pictures, and other forms and, therefore, has a significant composite characteristic in the form of expression. DU Wei and others also put forward the massiveness of electronic evidence.¹³ With the continuous increase of network bandwidth, the data generated in computer systems and networks every day are complex and massive. How to identify the electronic evidence related to the case and reflecting the objective facts of the case from the massive data is also a difficult task.

Regarding the collection of electronic evidence, the relevant party, mainly through the real-time monitoring and analysis of network data flow, audit trail, host system log, etc, detects the intrusion behavior to the network system and identifies, saves, and legally submits the digital evidence.¹⁴ Therefore, the sources of electronic forensics mainly include system logs, intrusion detection systems, firewalls, FTP, anti-virus software logs, e-mail, and card connecting equipment (including all kinds of modems, network cards, routers, and hubs). At present, electronic forensics technology shows the trend of integration, intelligence, and automation. The main technologies include IP address acquisition technology, IDS (Intrusion Detection System) forensics technology, massive data forensics technology based on data mining, automatic forensics technology in a collaborative environment, data recovery technology, data analysis technology, and data

12 Lingling Zhou, ‘Overview of Electronic Evidence and Its Collection and Identification’ (*China Court*, 7 December 2012).

13 Wei Du, Jianxin Peng and Li Mao, ‘Overview of Internet Electronic Evidence Collection Technology’ (2011) 2 *Forensic Science and Technology* 54.

14 ‘How to Lock Black Hands in Electronic Forensics in Big Data Era’ (*Legal Daily*, 22 September 2017) <<http://www.xinhuanet.com/>> accessed 15 April 2023.

preservation technology.¹⁵ With the development of the Internet and computer technology, electronic data collection, examination, and judgment have become basic and common work in criminal justice activities. However, the current electronic forensics technology still has great limitations and is difficult to meet the objective requirements of society and judicial practice for electronic forensics. For example, the market demand space for public cloud computing driven by big data and artificial intelligence makes data increasingly migrate from terminal devices to the cloud. At the same time, many cyber-related crimes also migrate to the cloud. Electronic forensics in the cloud environment has gradually increased. For example, how to collect cloud platform data, how to analyze the data, and how to locate data in the collection. For another example, IP on the cloud is not necessarily real IP and involves jurisdiction issues. In addition, since cloud storage data will be released at any time after use, how to fix it also poses a problem.

2.2 Blockchain characteristics and relevant laws and regulations

The government departments paid attention to the blockchain when it emerged in China. In 2013, the government departments noticed the risks of blockchain tokens and carried out relevant rectification work. In October 2016, under the guidance of the Ministry of Industry and Information Technology (MIIT), the China Blockchain Technology and Industrial Development Forum released the White Paper on China Blockchain Technology and Application Development which is the first technical document of blockchain under the guidance of the government.¹⁶ Since then, the MIIT has actively promoted the development of core technologies and standards of blockchain, marking that blockchain technology as a whole has entered the government's vision of governance. At present, a legal and regulatory system has been initially formed to regulate the blockchain, including laws, administrative regulations, departmental rules, other normative documents, and relevant policy documents. Specifically, there mainly are the Cybersecurity Law¹⁷, Criminal Law¹⁸, Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security (Amendment 2019)¹⁹, Decision of the Standing Committee of the National People's Congress on Strengthening the Protection

15 Wei Du, Jianxin Peng and Li Mao (n 13) 58.

16 'White Paper on Application of Blockchain Technology' (*Institute of Internet Industry*, 19 December 2018) <<https://wxappres.fecyan.com/block/report240/240.pdf>> accessed 15 April 2023.

17 Cybersecurity Law of the People's Republic of China 2016, art 22.

18 Criminal Law of the People's Republic of China 2023, arts 253, 286 and 287.

19 Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security 2019, art 7.

of Internet Information²⁰, Regulations of the People's Republic of China on the Security Protection of Computer Information Systems²¹, Measures for the Administration of Internet Information Services²², Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts²³, and Provisions on the Administration of Blockchain Information Services²⁴. Generally speaking, the legal, regulatory, and policy system of blockchain in China can be divided into two parts: one is to encourage technological exploration and standardize technological application; and the other is to strengthen the information security management of the blockchain network.

Regarding the characteristics of the blockchain, Wang Yuandi and others proposed that the blockchain has the main advantages of decentralization, distrust, traceability, collective maintenance, security and non-comparability, openness, anonymity, etc.²⁵ Wang Faming and others proposed that decentralization is the core advantage of blockchain. Decentralization refers to the decentralized distributed structure.²⁶ The whole network has neither centralized hardware or organization nor a centralized core system, which saves a lot of intermediary costs in reality. This is also one of the most important reasons for the wide application of blockchain. Specifically, the blockchain is a distributed database ledger, and transaction information data are stored in public ledgers on various nodes. Distributed ledgers are jointly maintained and synchronized in real-time (via network broadcasting) by multiple nodes, while account dealing rules based on complex cryptographic algorithms (Hash algorithm, etc) must be followed at the same time. The rights and obligations of all nodes in the system are the same, and the failure at any node will not affect the integrity of the system. It has the characteristics of distributed accounting, distributed propagation, and distributed storage. Regarding the non-comparability of blockchain information, Jesse and others mentioned that each node in the system has a complete database.²⁷ One has to control 51% of the nodes at the same time to falsify transaction data in the network, otherwise, the data tampering of individual nodes will not affect the data of other nodes, and the integrity and correctness

20 Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Internet Information 2012, art 2.

21 Regulations of the People's Republic of China on the Security Protection of Computer Information Systems 2011, art 5.

22 Measures for the Administration of Internet Information Services 2021, art 1.

23 Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, art 11.

24 Provisions on the Administration of Blockchain Information Services 2019, art 1.

25 Yuandi Wang, Li Li and Die Hu, 'Review of Blockchain Studies' (2018) 3 Journal of China University of Mining & Technology 75.

26 Faming Wang and Meijuan Zhu, 'Bibliometric Analysis of Domestic Hot Spots in Blockchain Research' (2017) 12 Journal of Intelligence 70.

27 Yli-Huumo and others, 'Where is current research on blockchain technology? A systematic review' (2016) 11(10) PLoS ONE e0163477.

of the entire ledger in the system will not be affected. Lin Xiaochi and others pointed out that traceability means that timestamp technology is adopted on the blockchain to add time dimension to the data and record the order of transactions, making the data traceable and easy to supervise and track.²⁸ Zhang Rui pointed out that the essence of de-trust is that the system converts the previous ‘trust in humans’ into ‘trust in machines’, that is, the blockchain grants credit with technical rules.²⁹ The trust granted does not come from the endorsement of a third party but the recognition of a consensus mechanism by all participants. In this way, the blockchain changes the previous contract and trust mechanism and realizes the exchange of trustworthy values, which will greatly reduce the dishonest behavior in the contract. Ma Ang and others put forward that collective maintainability means that the data in the system are collectively maintained by all participating nodes with maintenance functions, and anyone can participate. At the same time, the fault of any node will not affect the operation of the whole system, thus ensuring the stable operation of the whole system.³⁰

2.3 Legal effect of blockchain data as e-evidence

Legislation recognizes the validity of blockchain data as electronic evidence. Evidence validity of electronic data has experienced a period of development in China from scratch, from conceptualization to specific operating procedures for implementation. In 2002, the Supreme People’s Court issued the Provisions of the Supreme People’s Court on Several Issues Concerning Evidence in Administrative Proceedings, of which art 64 stipulates that electronic evidence shall have the same evidential effect as the original, but has not yet been defined as a statutory type of evidence.³¹ For example, previously in the process of hearing securities administrative cases, electronic data evidence such as electronic transaction information, network IP address, communication records, and e-mail were of vital importance in securities administrative cases due to the electronic, network-based, and wireless characteristics of securities transaction and information transmission. In 2011, the Supreme People’s Court promulgated the Summary of the Symposium on Several Issues Concerning Evidence in Hearing Securities Administrative Punishment Cases. The summary specifically stated that “due to the characteristics of electronic data evidence such as

28 Xiaochi Lin and Qianwen Hu, ‘Review of Research on Blockchain Technology’ (2016) 2 Financial Market Research 100.

29 Rui Zhang, ‘Traditional Financial Reform and Innovation Based on Blockchain’ (2016) 10 Southwest Finance 15.

30 Ang Ma, Xiao Pan and Lei Wu, ‘Summary of Research on Blockchain Technology Foundation and Application’ (2017) 11 Journal of Information Security Research 970.

31 Provisions of the Supreme People’s Court on Several Issues Concerning Evidence in Administrative Proceedings 2002, art 64.

diverse carriers, simple duplication, easy correction, deletion, and forgery, the requirements on the form of evidence and the verification of electronic data evidence should be stricter than other evidence methods.”³² Electronic data can only be submitted as evidence if it meets certain requirements. However, the Administrative Procedure Law of the People’s Republic of China was amended in 2014 to include the category of electronic data in the provisions of art 33 on types of evidence.³³ It is recognized from the legal level that electronic data can be used as the basis for determining the facts of a case if verified by the court. Subsequently, art 8 of the Electronic Signature Law revised in 2015 also stipulates the factors that should be considered for the authenticity of electronic data as evidence.³⁴ As a decentralized electronic data retention technology, blockchain has the characteristics of openness, distribution, and irreversibility. The data retained through blockchain technology are still electronic and fall within legal data types and, therefore, can be submitted and used as evidence materials in the administrative trial process.

The judicial interpretation clarifies the validity of blockchain data as electronic evidence. On the technical level, the distributed IT architecture of the blockchain has the characteristics of decentralization, transparency and openness, consistent state, and high dependence on cryptography. At the data level, the blockchain can keep the data consistent based on multi-party consensus, prevent data from being tampered with, and trace the whole process of data-based applications.³⁵ Based on this technical feature, blockchain technology is highly suitable for the preservation and authenticity examination of electronic evidence. At present, the examination and judgment of the authenticity of electronic data mainly rely on notarization procedures, which are formal examinations, complicated and cumbersome procedures, with weak probative force. The characteristics of Internet court cases, ie, online trials and a large amount of online evidence, objectively require breaking through the single way

32 Summary of the Symposium on Several Issues Concerning Evidence in Hearing Securities Administrative Punishment Cases 2011, s 2(1).

33 Art 33 of the Administrative Litigation Law of the People’s Republic of China 2017, “Evidence includes: (1) documentary evidence; (2) physical evidence; (3) audio and video recordings; (4) electronic data; (5) witness testimony; (6) statement of a party; (7) opinion of a forensic identification or evaluation expert; (8) survey transcripts and on-site disposition transcripts.”

34 Art 8 of Electronic Signature Law of the People’s Republic of China 2019, “The following factors shall be taken into consideration when making examination on the truthfulness of any data message as evidence: 1. The reliability of the methods for creation, storage or transmission of data message; 2. The reliability of the methods for keeping the integrity of the contents; 3. The reliability of the methods for identifying the addresser; 4. Other relevant factors.”

35 ‘Research Report on China’s Blockchain Technology and Application Development’ (*Chain Tower Think Tank*, December 2018) <http://pdf.dfcfw.com/pdf/H3_AP201804021115378434_1.pdf> accessed 15 April 2023.

of determining the authenticity through notarization procedures but making the substantive determination of the authenticity of electronic data through technical means and relevant supporting mechanisms.³⁶ In September 2018, the Supreme People's Court promulgated the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, which put forward clear standards for the authenticity review of electronic data and further explicitly recognized that blockchain can be used as technical methods for electronic data collection.³⁷

The recognition of blockchain data as effective evidence in trial practice. In judicial trial practice, before the promulgation of the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, Internet courts have begun to recognize the authenticity and reliability of blockchain technology in preserving electronic evidence. In June 2018, the Hangzhou Internet Court heard the case filed by *HuataiYimei Cultural Media Co., Ltd.* (hereinafter referred to as *HuataiYimei*) *v* *Shenzhen Daotong Science and Technology Development Co., Ltd.* (hereinafter referred to as *Daotong Technology*)³⁸ for the latter's violation of the former's right of online works information communication, which was the first time that a Chinese court confirmed the legal effect of electronic evidence storage by blockchain technology. In this case, the plaintiff HuataiYimei took screenshots of the web page where Daotong Technology published the infringing art, obtained the source code of the web page, packed and compressed the operation log, call time record, and other contents, calculated the hash value and uploaded it to FACTOM blockchain and Bitcoin blockchain for electronic data storage. According to the account number and password submitted by HuataiYimei, the Hangzhou Internet Court downloaded the preserved file package from www.baoquan.com. The web page contained therein showed that ladyfirst.com.cn had published the alleged infringing art. Upon examination, the body part was the same as the art involved in the case. The source code operation of the web page shows that the source code is www.ladyfirst.com.cn. Upon inquiry, the filing body of the website is Daotong Company. Through calculating the hash value of the preserved file package, and inquiring according to the inquiry methods and steps of the FACTOM blockchain and Bitcoin blockchain provided by Chain Forensic Science, it can be seen that the hash value exists in the blockchain, and the uploading time and the file package forming time are reasonable. According to the blockchain

36 Hu Shihao, He Fan and Li Chengqi. 'Understanding and Application of Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts' (2018) 28 People's Judicature 'Application, 24.

37 Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, art 11.

38 *HuataiYimei Cultural Media Co., Ltd. v Shenzhen Daotong Science and Technology Development Co., Ltd.* [2018] Hangzhou Court of the Internet Z 0192 Ming Chu No.81.

mechanism, it is known that the involved electronic evidence has been uploaded to the blockchain for preservation and has not been modified.³⁹ The judge of Hangzhou Internet Court held that the legal effect of this electronic evidence storage method should be comprehensively recognized based on the principles of technical neutrality, technical explanation, and case review in practical trials. Neither should the identification standard be excluded or improved because the blockchain and other technologies are new and complicated technical means at present, nor should the identification standard be lowered because of the technology's tamper and deletion-proofing features, but its evidence effect should be comprehensively judged according to the relevant legal provisions on electronic data. Because of the blockchain's tamper and deletion-proofing features, it is reliable as a method of maintaining content integrity after confirming that the contested electronic data has been saved in the blockchain. In October 2018, in the case filed by *COL Digital Publishing Group Co., Ltd. v Beijing Jingdong 360 Degree Electric Commerce Co., Ltd.*⁴⁰ for the latter's infringement upon the former's online works information communication, Beijing Dongcheng District Court held as follows in terms of the integrity and method reliability of electronic data preserved in the blockchain: after evidence collection through a third-party storage platform, the platform automatically generated a unique corresponding and encrypted digital fingerprint (hash value), and then generated a data preservation certificate containing hash value, blockchain security ID, time of evidence collection and other information, thus ensuring the integrity of electronic data. On 24 January 2019, in a case filed to the *Beijing Internet Court over right of online works information communication among Beijing Microlive Vision Technology Co., Ltd. vs Baidu Online Network Technology (Beijing) Co., Ltd. and Beijing Baidu Netcom Science and Technology Co., Ltd.*,⁴¹ the plaintiff provided its evidences, including ICP filing information inquiry, screenshots of the homepage of Tik Tok website, screenshots of the developer information of Tik Tok APP (Android system and iOS system), authorization letter issued by XIE, (2018) Jing Dong Fang Nei Min Zheng Zi No 10028 Notarial Deed, (2018) Yue Guang Nan Yue No 8614 Notarial Deed, the screenshots of developers' information of HuoPai APP (Android system and iOS system) and the corresponding blockchain certificate of evidence, the screenshots of web page showing 'the total participation of the national party media platform in interactive activity of commemorating

39 Yichun Lu, 'Determination of Legal Effect of Blockchain Electronic Evidence' (IPLEAD, 2 December 2018) <<https://www.zhichanli.com/>> accessed 15 April 2023.

40 *COL Digital Publishing Group Co., Ltd. v Beijing Jingdong 360 Degree Electric Commerce Co., Ltd.* [2018] Dongcheng District Court J 73 Ming Zhong No.2163.

41 *Beijing Microlive Vision Technology Co., Ltd. vs Baidu Online Network Technology (Beijing) Co., Ltd. and Beijing Baidu Netcom Science and Technology Co., Ltd.* [2018] Beijing Internet Court J 0491 Ming Chu N0.1.

the “5.12” exceeds 600 million’ and blockchain certificate of evidence, and the evidences were accepted by the courts.

The construction of the judicial blockchain of Internet court promotes the credibility of the whole process of electronic evidence. In addition to adopting blockchain data as electronic evidence in specific cases, Hangzhou Internet Court and Beijing Internet Court have respectively promoted the construction of judicial blockchain for the preservation of electronic evidence in copyright protection, contracts, financial disputes, and other fields, and promoted the production, storage, dissemination, and use of electronic data to realize credibility of the whole process.⁴² The judicial blockchain constructed by Hangzhou Internet Court consists of three layers: first is blockchain procedure, through which users can directly record the entire process of operation in the blockchain, such as online submission of electronic evidence such as electronic contracts, rights protection process, and service process details; second is the full link capability layer of the blockchain, which mainly provides credibility service of real name authentication, electronic signature, timestamp, data storage, and the whole process of the blockchain; third is the judicial consortium layer, which connects notary offices, CA/RA institutions, judicial authentication centers and courts with blockchain technology, with each unit becoming a node in the chain.

To sum up, more and more cyber-related crimes are migrating to the cloud, which increases the difficulty of electronic evidence collection. As electronic evidence, blockchain data has legal effect. At the same time, the advantages of blockchain, such as de-centralization, de-trust, traceability, collective maintenance, security, non-comparability, openness, and anonymity exactly solve the problems of intangibility, vulnerability, and other characteristics of electronic evidence. The importance of the construction of a blockchain electronic evidence collection system is evident. For example, given the traceability of blockchain, timestamp technology is adopted to ensure the traceability, integrity, and non-comparability of data, thus addressing the intangibility of electronic evidence. For another example, given the security feature of the blockchain, the data is encrypted with the encryption technology to ensure the security of the data, plus the strong calculation capacity formed by consensus algorithm, to resist external attacks and ensure non-comparability and unforgeability of the blockchain data, thus solving the vulnerability problem of electronic evidence. However, the application of blockchain electronic evidence storage is still a new thing, and the research on the application of blockchain characteristics in the collection and preservation of electronic evidence is very weak at home and abroad. This paper is to make up for this loophole.

42 ‘White Paper on Application of Judicial Evidence Stored on Blockchain’ (*Information Center of the Supreme People’s Court*, 8 June 2019) <<http://www.caict.ac.cn/>> accessed 15 April 2023.

3. Case analysis of blockchain evidence

The arbitration chain is established based on the underlying open-source platform of the FISCO BCOS blockchain. FISCO BCOS is an underlying open-source blockchain platform tailored for the financial industry with financial business practices as a reference sample and a financial branch version of the BCOS open-source platform created under the leadership of several members of the FISCO open-source working group such as WeBank, Shenzhen Securities Communication Co., Ltd., and Tencent Cloud. FISCO BCOS provides a comprehensive supervision and audit support module, including access control, CA identity authentication, account management system, and security monitoring, to support mass data capacity storage and flexible expansion. It also has the key management mechanism and privacy protection mechanism to fully meet the technical requirements of evidence storage in arbitration.⁴³

3.1 Working principle of arbitration chain

The arbitration chain is governed in a consortium blockchain way. Figure 1 shows the business architecture diagram of the arbitration chain.⁴⁴ In this network, WeBank, evidence storage institutions, arbitration institutions, and other related parties can join as chain nodes to form a reliable consortium chain network.

43 'Arbitration Chain: Evidence Storage Practice Based on Blockchain' (*WeBank*, 2 October 2017) <<https://fisco-bcos-documentation.readthedocs.io/zh-cn/release-1.3/docs/applications/%E4%BB%B2%E8%A3%81%E9%93%BE%EF%BC%9A%E5%9F%BA%E4%BA%E5%8C%BA%E5%9D%97%E9%93%BE%E7%9A%84%E5%AD%98%E8%AF%81%E5%AE%9E%E8%B7%B5/README.html>>

44 *ibid.*

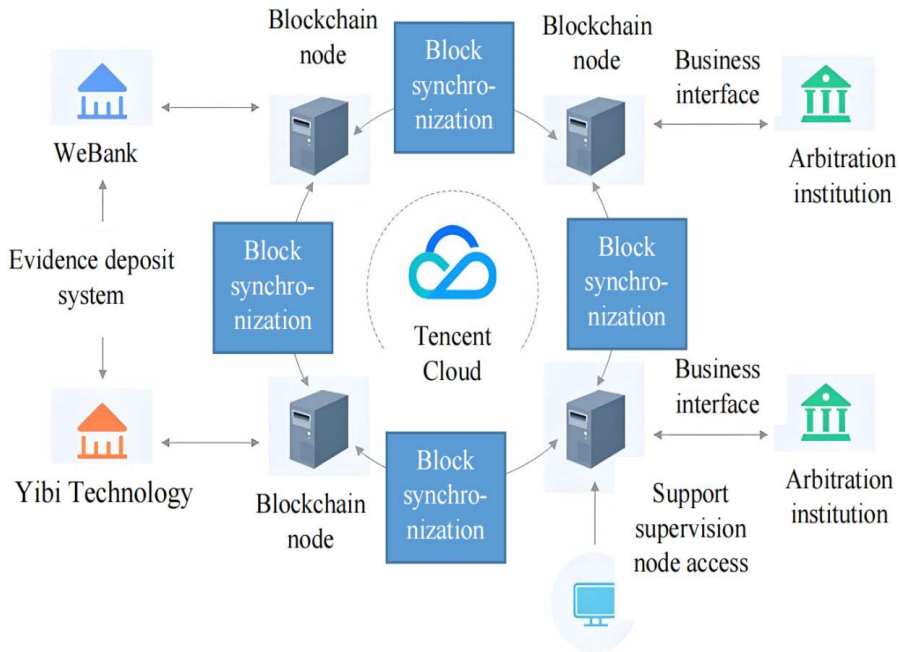


Figure 1. The business architecture diagram of the arbitration chain. Source: Arbitration Chain: Evidence Storage Practice Based on Blockchain (fisco-dev, 21 June 2019), at <www.bookstack.cn/read/fisco-bcos-v1.3/9c02182012f53485.md> (translated by the authors).

The arbitration chain adopts a governance method that conforms to the characteristics of the arbitration business to ensure good security features and privacy protection capabilities in its business setup, and in-depth research is conducted on how to clearly and conveniently monitor the operation status of the consortium chain, and support supervision and auditing demands, to ensure that the requirements of the financial industry on data structure, visualization, supervision, and auditing are met. Specifically: 1) only permitted members are allowed to join, thus avoiding the hidden danger of data leakage caused by irrelevant members joining the chain; 2) the consortium chain has a good management mechanism enabled by a variety of mechanisms such as joint governance, legal organization governance, leadership member governance to deal with various problems and optimize the management process; 3) each participant can be assigned with different operation privileges and their responsibilities clearly defined to prevent data privacy from being leaked to inappropriate members; 4) the activities on the chain can be monitored in real-time and abnormal activities intervened by setting up independent observation nodes, calling API data interfaces, deploying specific intelligent contracts, etc. Blockchain browser, monitoring system, monitoring node, and anti-money laundering interface are all the

implementation links of governance. Specifically, 1) the arbitration chain provides a blockchain browser, which can visualize the data on the blockchain and display it in real-time. Users can easily obtain the deployed blockchain nodes, blocks, and transaction information through the web page even if they have no technical background; 2) the monitoring statistics log is optimized to enable developers to quickly obtain important parameters in the running process of the blockchain system and evaluate the running state of the system from multiple dimensions; 3) the supervisory or auditing department can be integrated as a special supervisory node, so that they can synchronize data in real-time and monitor or audit the integrity and validity of the data, and can also carry out compliance inspection of business processes, anti-money laundering and other operations at the same time.

3.2 Workflow of arbitration chain

The application of electronic evidence in the arbitration chain mainly includes three parts: evidence storage, evidence collection, and evidence authentication. Evidence storage is the core part. Before initiating storage, an intelligent contract of initial conditions for storage shall be deployed to stipulate the conditions required for the evidence storage to take effect. Fig. 2 is a schematic flow chart of evidence storage. In the so-called evidence storage, business data is uploaded after being signed by the WeBank evidence storage system, and the evidence storage institution and arbitration institution are notified to confirm the data signature after successful uploading. After receiving the notice, the evidence storage institution and arbitration institution will take out the data uploaded onto the chain to verify and sign, thus completing the whole storage process. In the whole process of storage, the intelligent contract guarantees that no party can change the data stored, but only can add data to the stored data. Meanwhile, the quasi-real-time asynchronous upload of the evidence storage system does not influence the normal business logic. The evidence storage business process includes five steps: first, all parties involved in the storage need to agree on the conditions required for the storage to take effect in advance, and then one party will call SDK API to create and deploy a factory contract, which will come into effect through consensus; secondly, the storage business party calls the factory contract through SDK API to create a new evidence contract with its signature; thirdly, the storage institution calls SDK API to sign and confirm the evidence; fourthly, the arbitration institution calls SDK API to sign and confirm the evidence; finally, the arbitration institution obtains the evidence information on the chain through SDK API, and verifies the correctness and completeness of the existing signature of the evidence.

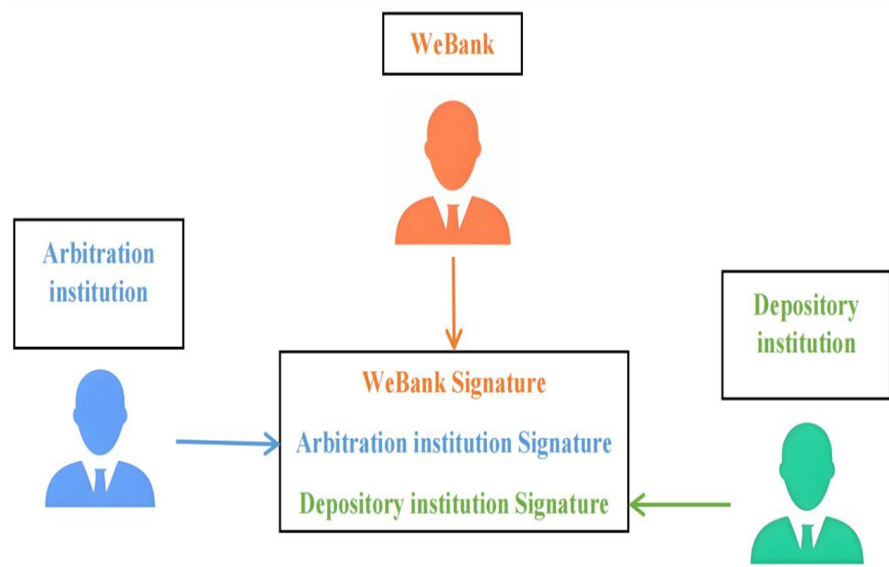


Figure 2. Schematic flow chart of evidence storage. Source: Arbitration Chain: Evidence Storage Practice Based on Blockchain (fisco-dev, 21 June 2019), at www.bookstack.cn/read/fisco-bcos-v1.3/9c02182012f53485.md (translated by the authors).

For evidence collection, when there is a need for evidence collection, WeBank selects data from the arbitration chain and submits the data to the arbitration institution. The arbitration institution analyzes the data provided by WeBank to obtain the relevant address information of the blockchain, and then retrieves the data on the chain through the address; finally, in blockchain authentication, the arbitration institution calls the related SDK interface after obtaining evidence to judge whether the evidence storage meets the initial conditions for the storage to take effect.

3.3 Application Effect of Arbitration Chain

The arbitration chain is based on a multi-centralized, tamper-proof, and trustworthy blockchain. With distributed data storage, encryption algorithms, and other technologies, the transaction data is signed with consensus and uploaded, the real-time preserved data forms the evidence chain through intelligent contracts to meet the requirements of authenticity, legality, and relevance of evidence and realize standardized evidence and trial.⁴⁵ In February 2018, the

⁴⁵ Wanyun Shao, 'Guangzhou's First Arbitration Chain Judgment Released' (*China Economic*, 13 March 2018) <http://m.ce.cn/cj/gd/201803/13/t20180313_28446837.shtml> accessed 15 April 2023.

Guangzhou Arbitration Commission announced the feasibility of the arbitration chain in the industry's first award issued based on the arbitration chain. Since the release of the arbitration chain, more than 10 evidence storage institutions and arbitration institutions have joined the arbitration chain ecology. As of the fourth quarter of 2018, more than 10 million contracts have been stored, involving a capital scale of 100 billion yuan.⁴⁶

After being applied in the arbitration industry, the blockchain has played a very important role in the collection of judicial evidence because of its traceability of records. A trustworthy blockchain network is currently incorporated into our transactions to complete the fixation and uploading of evidence in real-time. At the same time, it also allows the judicial institutions to participate in the bookkeeping of the blockchain and connect with the network arbitration tribunal to form a fast dispute resolution channel. With the establishment of the smart city, the city's transaction information will be recorded on the transaction chain in real-time. During evidence collection for judicial arbitration, it enables rapid trace back directly through the blockchain, and at the same time ensures the authenticity of the information, thus avoiding the step of evidence authentication and saving a lot of human resources. In addition, in the trial of cases involving over 2000 yuan to 50000 yuan, the lawyer's fees and travel costs are about 2000 yuan. If the online trial is adopted, the judicial cost is greatly reduced to only 500 yuan. Regarding the trial cycle, it, generally takes more than 6 months or even 1 year to complete filing, hearing, and delivery, while online arbitration only takes 7 to 15 days.⁴⁷ Specifically, when a default occurs and a party needs to apply for arbitration, it only needs to click 'One-key Arbitration' in the back-end system, and the data of the default transaction will be restored to the original data and sent to the arbitration platform of the arbitration commission. After receiving the original data, the arbitration commission will compare it with the previously stored data and issue an arbitration award after confirming the authenticity and integrity of the data. The time taken from clicking 'One-key Arbitration' to receiving the arbitration award can be as short as 7 days. At the same time, the arbitration fee can be as low as 500 yuan to 600 yuan for each transaction.⁴⁸ For arbitration institutions, the arbitration chain ensures that the transaction information on the chain will not be tampered with and helps arbitration institutions to quickly authenticate evidence, resolve disputes, reduce the labor, material, and time costs in the arbitration process, improve judicial

46 'China Blockchain Technology and Application Development Research Report' (*China Environmental Library*, 18 December 2018).

47 Yiming Liu, 'Public Consortium Chain Is the Key to the Door of Distributed Business Model' (*China Technology*, 8 June 2021).

48 *ibid.*

efficiency, and reduce overall arbitration costs.⁴⁹ For the parties involved, the arbitration chain will quickly and effectively resolve disputes and improve the operation and risk control efficiency.⁵⁰

It can be seen that the application of the objective and transparent blockchain technology and operation mechanism makes the evidence or contracts more disaster-tolerant, reliable, and fault-tolerant, thus avoiding many expenses arising from conflicts and disputes, effectively reducing the risks of manual operation and moral hazard, and effectively solving the pain points of difficult evidence collection and arbitration. Moreover, through the arbitration chain, the arbitration institution can participate in the process of the evidence storage business, and together reach a consensus and witness in real time. In case of disputes, the signed and authenticated evidence storage data can be taken as direct evidence, to greatly reduce the arbitration process, help the arbitration institution to quickly complete the authentication of evidence and quickly resolve disputes, to further improve judicial efficiency, and reduce arbitration costs. At the same time, it is also conducive to maintaining law enforcement transparency, judicial justice, and social harmony.

49 According to the China International Commercial Arbitration Annual Report (2017) issued by the China International Economic and Trade Arbitration Commission on 16 September 2018, in 2017, 253 arbitration commissions nationwide accepted and heard 239,360 cases, an increase of 30,815 cases or 15% over 2016. Each arbitration commission received 946 cases on average, an increase of 115 cases or 14% over 2016. Among them, 6 arbitration committees handled 85,399 cases through online arbitration, accounting for 36% of the total number of cases nationwide. These data not only show that the arbitration chain has a huge market in China, but also play an important role in easing the work pressure of the arbitration commission. See China International Economic and Trade Arbitration Commission, 'China International Commercial Arbitration Annual Report (2017)' (China International Economic and Trade Arbitration Commission official website, 16 September 2018) <<http://www.cietac.org/>> accessed 15 April 2023.

50 The China Arbitration Credibility Evaluation Report (2018) shows that 20.14% of the parties chose arbitration because of its high efficiency, 15.56% because of its professionalism and 15.00% because of its fairness. It can be seen that one of the important factors for the parties to choose arbitration to resolve disputes is that arbitration is usually more efficient than litigation and can more smoothly stop loss in a timely manner. For example, both the CIETAC and the Beijing Arbitration Commission decide domestic arbitration cases within 4 months and international arbitration cases within 6 months from the date of the court organizing. The use of arbitration chain for arbitration greatly shortens the duration and facilitates rapid resolution of disputes by the parties. See China University of Political Science and Law, 'China Arbitration Credibility Evaluation Report (2018)' (China University of Political Science and Law Newspaper Website, 11 June 2019) <https://newspaper.cupl.edu.cn/index/article/articleinfo?doc_id=8142> accessed 15 April 2023.

4. Problem analysis of blockchain evidence and its authenticity

4.1 Security risks at the technical level

The transmission and storage of blockchain data are open to the public, which is the advantage of blockchain-distributed bookkeeping, but at the same time, it also makes security threats the most significant problem faced by blockchain. For the application of blockchain electronic evidence involving a large number of personal privacy, business secrets, and even state secrets, unsafe data do not meet the legal standards for the identification of evidence. At this point, the evidence will become worthless. From the perspective of blockchain security analysis, the challenges come from algorithm security, protocol security, and cryptography security.⁵¹

4.1.1 Algorithm security risks

At present, there has not been any mainframe (super) computer serving as the node of the blockchain network. With the development of computational mathematics, cryptography, and computational capability, the blockchain will soon face the possibility of the algorithm being cracked.⁵² Once the main data link is cracked, all the data will never be recovered. In April 2017, a foreign organization cracked 30 Bitcoin wallets with 3,000 trillion keys. In addition, as quantum computers become possible, the asymmetric encryption algorithm used in the blockchain in the future may be cracked by hackers, which is a potential security threat to the algorithm that the blockchain technology has to face.⁵³

4.1.2 Protocol security risks

Blockchain technology is based on POW and other consensus mechanisms and its security risk lies in the 51% computing power attack. When a blockchain node is passed by a computer with more than 51% computing power, it can successfully tamper with and forge blockchain data.⁵⁴ Although no organization or institution has mastered 51% computing power at present, due to the uneven distribution of ore pools and miners, some ore pools have enough computing power to have administration privileges to some extent. If these large ore pools are broken through, 51% of the network nodes will be controlled by malicious

51 Yuandi Wang, Li Li and Die Hu (n 25) 81.

52 Jian Zhang, *Blockchain: Defining the Future of Finance and Economics* (China Machine Press 2017).

53 'Is bitcoin secure? The organization cracked 30 wallets with 3000 trillion ciphers' (*Chain Node*, 10 July 2019).

54 Yong Yuan and Feiyue Wang, 'Development Status and Prospect of Blockchain Technology' (2016) 4 *Acta Automatica Sinica* 481, 494.

people, then tampering and forgery of blockchain information will become completely possible, the authenticity of electronic evidence will be seriously questioned, and blockchain electronic evidence storage will be meaningless.

4.1.3 Password cracking vulnerability

Any cryptography is relatively safe. With the improvement of computing methods and power, the probability of cryptography being cracked becomes increasingly higher. Cryptography is relatively safe in a certain period, but it can hardly be safe in the long run.⁵⁵ Blockchain which uses a large number of cryptographic methods is a highly algorithm-intensive project with the computer capability at risk of being cracked on a large scale at present. GSM and WCDMA communication air interface encryption method is considered to be the most unlikely to be cracked (Encryption with snow), but it has been cracked by scholars from Israel and other countries in just ten years. Once the encryption algorithm is cracked, the entire security foundation of the blockchain will no longer exist, and all kinds of data will be exposed to the public. Electronic evidence involving personal privacy, trade secrets, and even state secrets, in particular, will bear the brunt.

4.2 Regulatory issues

After the Guangzhou Arbitration Commission issued the industry's first award based on the arbitration chain in February 2018, at 10:00 am on 28 June 2018, the judgment of the first blockchain evidence storage case in China was pronounced in the Hangzhou Internet Court which supported the plaintiff's adoption of blockchain as the evidence storage method and confirmed the corresponding infringement facts. On 7 September 2018, the Supreme People's Court also promulgated the Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts, formally acknowledging the binding force of blockchain evidence in addressing legal disputes.⁵⁶ However, in the judicial practice at present, there are still problems in the identification of the evidence authenticity and the lack of a unified and practical standard.

4.2.1 Authenticity problem of blockchain evidence

Blockchain electronic evidence storage mainly authenticates data with the timestamp function of blockchain technology and 'anchor technology'. To put its technical principle simply, it records and stores the data that appears and

55 Xin Shen, Qingqi Pei and Xuefeng Liu, 'Overview of Blockchain Technology' (2016) 11 Chinese Journal of Network and Information Security 11, 20.

56 Provisions of the Supreme People's Court on Several Issues Concerning Cases Trial by Internet Courts 2018, art 11.

exists at a certain moment on the blockchain through encryption protection (including electronic contracts, web screenshots, computer documents, video files, call records, and other electronic ‘source files’), and affixes timestamp on the data to ensure the originality, integrity, and non-comparability of the data, thus realizing the self-authentication of the data. In the above-mentioned copyright dispute case heard by Hangzhou Internet Court, to prove that the defendant Daotong Technology published on its website the related works over which the plaintiff had copyright, the plaintiff HuataiYimei automatically called Google open source program puppeteer to capture the pictures of the infringing web pages, and at the same time called curl to obtain the source code of the target web pages, and calculated the compressed packages of the two and the called logs into Hash and uploaded them to FACTOM blockchain and Bitcoin blockchain. The arbitration chain currently in use by the Guangzhou Arbitration Commission is based on a multi-centralized, tamper-proof, and trustworthy blockchain. With distributed data storage, encryption algorithms, and other technologies, the transaction data is signed with consensus and uploaded, the real-time preserved data forms the evidence chain through intelligent contracts. According to the provisions of the Civil Procedure Law, authenticity, legality, and relevance are the criteria and principles for judging whether evidence has legal effect. In the aspect of examining the legal effect of blockchain electronic evidence storage, Hangzhou Internet Court examined and demonstrated the legal effect of the blockchain electronic evidence storage involved in the case in terms of the authenticity of the electronic data source, the reliability of storage, the integrity of content and the degree of correlation with other evidence, and finally determined that the blockchain electronic evidence submitted by the plaintiff has legal effect. However, in the first award based on ‘blockchain + evidence storage’ made by the Guangzhou Arbitration Commission, the electronic evidence storage of the blockchain involved in the case was directly determined to be legal and valid,⁵⁷ but its authenticity was not analyzed. The award reflects a question, namely, whether the authenticity of the electronic evidence storage of the blockchain can be directly determined on the premise that there is no evidence to the contrary to overturn it.

On 7 September 2018, the Supreme Court issued the Provisions of the Supreme People’s Court on Several Issues Concerning Cases Trial by Internet Courts, of which art 11 is the provision on judging the authenticity of electronic data.⁵⁸ The provision stipulates that when judging the authenticity of electronic

57 MA Ce, ‘From electronic evidence storage to blockchain evidence storage, where is the imagination space of judicial effect’ (*Zhibu Website*, 19 March 2018) <<https://zhuanlan.zhihu.com/p/34711967>> accessed 15 April 2023.

58 Art 11 of Provisions of the Supreme People’s Court on Several Issues Concerning Cases Trial by Internet Courts 2018, ‘If a party raises any objection to the authenticity of electronic data, an Internet court shall, in light of the cross-examination information, examine and judge the

data, the court needs to examine the authenticity of the process of electronic data generation, collection, storage, and transmission, and emphasizes the importance of examining the cleanness of the electronic data environment, the clarity of the subject and time, the accuracy and non-comparability of the content. In addition, para 2 of the provision specifically stipulates that ‘the Internet court shall recognize electronic data submitted by the parties if the authenticity of the data can be proved by technical means of collection, fixation, and anti-tampering of such evidence as electronic signature, trustworthy timestamp, hash value check, blockchain or proven through electronic evidence collection and storage platform’, which means that the blockchain evidence fixation and storage technology has received judicial confirmation for the first time in China and its application at the judicial level ushered in a breakthrough. At the same time, some people think that even though para 2 makes special provisions on evidence storage and fixation with the blockchain technology, the authenticity of the electronic evidence collected and fixed with this technology should be examined following the methods and principles specified in para 1, instead of regarding the data as authentic for granted.

In addition, according to art 9 of the Provisions of the Supreme People’s Court on Evidence in Civil Proceedings,⁵⁹ it is not necessary for the parties involved to prove well-known facts, natural laws and theorems, and facts that have been proved by valid notarization documents. One of the major reasons is that these facts are objective facts or legal facts, which are regarded as real with no dispute in law. As the data recorded in the blockchain are true, the facts recorded and reflected in the data, including transaction behaviors, should also be true. Whether the parties involved need to prove such facts is also worth considering.

authenticity of the generation, collection, storage and transmission process of the electronic data, with the focus of examination put on the following: (1) Whether the hardware and software environments such as the computer system based on which electronic data is generated, collected, stored and transmitted are safe and reliable. (2) Whether the generation entity and time of the electronic data are specified, and whether the contents shown are clear, objective and accurate. (3) Whether the storage and safekeeping media of electronic data are definite, and whether the safekeeping methods and means are appropriate. (4) Whether electronic data extraction and fixation entity, and electronic data extraction and fixation tools and methods are reliable, and whether the extraction process can be reproduced. (5) Whether the contents of electronic data are added, deleted, modified or incomplete, or fall under any other circumstance. (6) Whether electronic data can be verified in specific methods.”

59 Art 9 of Provisions of the Supreme People’s Court on Evidence in Civil Proceedings 2008, “The facts as mentioned below need not be proved by the parties concerned by presenting evidences: 1. The facts that are known by all people; 2. Natural laws and theorems; 3. The fact that can be induced according to legal provisions or known facts or the rule of experience of daily life; 4. The facts affirmed in the judgment of the People’s court that has taken effect; 5. The facts affirmed in the award of the arbitration organ that has taken effect; 6. The facts that have been proved in the valid notary documents.”

4.2.2 *Lack of the unified and practical standard for blockchain evidence*

At the current stage, if it is allowed to directly determine the authenticity of blockchain electronic evidence in judicial practice, there are still some problems. We know that notarization has been widely used in the field of judicial practice for a long time, with corresponding laws and regulations, guiding opinions, and industry rules, as well as a set of mature practical standards, and it is also easy for judicial personnel to understand. Therefore, the legal effect of notarization can be easily recognized by judicial personnel. Compared with notarization, one of the main problems faced by blockchain electronic evidence storage is the lack of a unified and practical implementation standard. At present, there is no uniform judicial approval standard for blockchain electronic evidence storage in the selection of third-party evidence storage platforms, technical standards for implementation, types of blockchains used, procedures and methods for evidence storage, standards for judicial review, etc. Because the legal effect of blockchain electronic evidence cannot be reviewed according to the established uniform standards and the fact that blockchain is a new technology, most judges do not know much about this technology, which will easily lead to inconsistent judgment standards and is not conducive to achieving fairness and justice in judgment results.

5. The USA blockchain evidence authenticity rules

5.1 How the USA treats blockchain evidence

In the USA, some states, as the pioneers of blockchain evidence rules, mainly adopt two methods to emphasize the principle of equal treatment.⁶⁰ The so-called equal treatment means that laws and regulations should treat blockchain evidence in the same way as existing legal forms of evidence. Also, the specific part of the blockchain evidence should be given the same treatment, and it will never be excluded or emphasized because it was born in a new technology environment. This principle was repeatedly stated when various new 'data messages' were born in the early years. For example, art 5 of the UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, 1996 with additional art 5 bis as adopted in 1998 stipulates: 'Information shall not be denied legal effect, the validity or enforceability solely because it is in the form of a data

60 Shelagh Dolan, 'How the Laws & Regulations Affecting Blockchain Technology and Cryptocurrencies, Like Bitcoin, Can Impact Its Adoption' (*Business Insider*, 3 March 2020) <www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global> accessed 15 April 2023.

message’.⁶¹ One is to separately stipulate the evidence status of blockchain records. For example, the Act relating to Recognizing the Validity of Distributed Ledger Technology of Washington 2019 stipulates: ‘Electronic records shall not be denied legal force, the validity or enforceability solely on the ground that they are generated, communicated, received or stored using distributed ledger technology’.⁶² The second is to stipulate its legal effect together with smart contracts and electronic signatures. As stipulated in the Blockchain Technology Act of Illinois,⁶³ which went into effect in January 2020, ‘Smart contracts, records or signatures shall not be denied legal validity or enforceability simply because they are created, stored or verified by the blockchain’, ‘Evidence of smart contracts, records or signatures created, stored or verified on the blockchain cannot be excluded in litigation’, ‘If the provision of signed material is required by law, the submission of signature data electronically recorded on the blockchain or blockchain evidence to verify the intent of the signer intended to provide this condition is also met’.

Relevant bills and laws in Arizona, New York, and Ohio have also made such adjustments. In March 2017, Arizona amended the state’s Revised Statutes by adding a new chapter on electronic transactions.⁶⁴ According to the newly added provisions, the signing behavior through the blockchain is regarded as a qualified electronic signature that meets the formal requirements, and the records and contracts obtained through the blockchain are deemed to meet the formal requirements and qualified records. Smart contracts may be used in commercial activities, and the legal validity, validity, or enforceability of the contract shall not be denied just because the contract contains smart contract terms. In January and March 2019, Bills No 1683 and No 4142 of the New York State Senate proposed amendments to the electronic signature and document law.⁶⁵ These two bills contain provisions to confirm that signatures and contracts can be made through the blockchain, as well as provisions to confirm the validity of

61 UN Commission on International Trade Law, ‘UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, 1996 with additional article 5 bis as adopted in 1998’ (United Nations Digital Library, 9 April 1999) <<https://digitallibrary.un.org/record/286739?ln=en&v=pdf>> accessed 15 April 2023.

62 Recognizing the validity of distributed ledger technology Act Washington Senate Bill 5638 2019, s 3.

63 The Blockchain Technology Act House Bill 3575 2020, s 10(a).

64 An Act Amending section 44-7003, Arizona revised statutes; amending title 44, Chapter 26, Arizona revised statutes, by adding article 5; relating to Electronic transactions House Bill 2417 2017.

65 An Act to amend the state technology law, in relation to blockchain technology and smart contracts Senate Bill 4142 2019; An Act to amend the state technology law, in relation to blockchain technology and smart contracts Assembly Bill 1683 2019.

smart contracts. In Ohio, Senate Bill 300,⁶⁶ introduced in May 2018, proposes to recognize smart contracts with full legal force and enforceability.

5.2 Commonalities in the blockchain evidence authenticity rules between the USA and China

On the one hand, both China and the USA generally apply existing rules on the authenticity of electronic evidence to blockchain evidence. In the USA, blockchain records fall under the broader category of electronic evidence.⁶⁷ In practice, ordinary electronic evidence can be applied to methods or rules such as insider testimony, check value verification, electronic record verification, judicial cognition, etc.⁶⁸ These methods or rules can also be used for blockchain evidence. In China, the representative rules on the authenticity of electronic evidence also be applied to blockchain evidence. For example, arts 93 and 94 of the Provisions by the Supreme People's Court on Evidence in Civil Procedures 2019⁶⁹ established a 'three-in-one' system of reasoning standards,⁷⁰ presumption standards, and cognitive standards for reviewing and judging electronic evidence. In practice, the blockchain records can completely follow the situations listed in the above provisions, making 'presumptions that are unfavorable to oneself', 'presumptions that originate from a neutral third-party platform', 'presumptions that are based on normal business records', 'presumption of archival storage', 'presumption of compliance with the agreement', etc.

Moreover, the above presumptions can usually be shared by multiple items for blockchain evidence. In the same way, the 'deemed as the original electronic data' rule implemented in my country can also be applied to blockchain evidence. For example, para 2 of art 15 of the Several Provisions on Evidence in Civil Litigation 2019⁷¹ stipulates: 'The copy made by the producer of electronic data that is consistent with the original, or the printout directly derived from electronic data or other output media that can be displayed and identified, shall be deemed as the original electronic data'. On the other hand, US federal laws and some state laws have made amendments to blockchain evidence for

66 A Bill to amend sections 1306.01, 1306.04, and 1306.06 of the Revised Code to amend the Uniform Electronic Transactions Act to define records and contracts secured by blockchain technology as electronic records and to allow the use of smart contract terms Senate Bill 300 2018.

67 Victoria Lemieux, 'Blockchain for Recordkeeping: Help or Hype' (ResearchGate, October 2016) <https://blogs.ubc.ca/recordsinthechain/files/2018/06/FinalReport_Volume1.pdf> accessed 15 April 2023.

68 Federal Rules of Evidence 2023, Rule 901(b)(1).

69 Provisions by the Supreme People's Court on Evidence in Civil Procedures 2019, arts 93 and 94.

70 Pinxin Liu, 'On the Authenticity Standards of Electronic Evidence' (2021) 1 Social Science Series 68.

71 Several Provisions on Evidence in Civil Litigation 2019, art 15.

authenticity rules, best evidence rules, and presumption rules. The Supreme People's Court has also introduced the Special Articles on the Authenticity of Blockchain Evidence in the Rules of Online Litigation of People's Court 2021.⁷²

5.3 Commentary on the USA blockchain evidence authenticity rules

Although the authenticity rules of blockchain evidence in the United States are subject to insufficient practical innovation, they also can provide many insights for enacting rules of blockchain evidence authenticity in China. This is prominently reflected in the legislation of some states by expanding the rules of 'self-authentication', 'presumption of business record exception', and 'presumption scope'. In June 2016, Vermont passed an act relating to miscellaneous economic development provisions, and a separate chapter sets out the provisions regarding the validation and admissibility of blockchain records in court.⁷³ The act stipulates that if an electronic record registered electronically on the blockchain is sworn to be supported by a qualified person through a written statement, it is self-authenticating. The relevant written statement must indicate that itself made the written statement, indicating that the date and time when the electronic record enters the blockchain, the electronic record is kept in the blockchain as a normal business activity, and the electronic record is processed following normal business activities in line with customary practices. Certainly, this presumption (self-authentication) does not mean that the facts of the case or the content of the records are true, valid, or legal. The Act, which has the same effect as the Vermont Rules of Evidence 2011,⁷⁴ affirms the admissibility of electronic records stored on a blockchain in a trial or hearing. In September 2019, Virginia proposed a provision titled 'Business Records, Electronically Registered on a Blockchain Self-authenticating document' as House Bill No 2415 to the State House of Representatives.⁷⁵ The Bill stipulates, 'In any civil litigation, where a business record electronically registered on a blockchain is substantive and admissible, it should be presumed to be self-authenticating and extrinsic evidence of its authenticity should no longer be required'. The Bill establishes the same presumption rules as those outlined in the Act mentioned above, specifically concerning the presumption of authenticity of the record, the date and time of the record, and the maker

72 Rules of Online Litigation of people's Court 2021, arts 16 to 19.

73 An act relating to miscellaneous economic development provisions House Act 868 2016.

74 Vermont Rules of Evidence 2011, Rule 1101.

75 A Bill to amend the Code of Virginia by adding a section numbered 8.01-390.4, relating to business records electronically registered on a blockchain self-authenticating House Bill 2415 2019.

of the record. New York, California, and other states have also imitated the Act and enacted similar regulations.⁷⁶

Looking at the above-mentioned state legislation in the USA, it is not difficult to find that the advantage of its blockchain evidence authenticity rules is that it is practically useful, and this is attributed to three consensuses. First, the focus of rule construction is the authenticity of the data after entering the chain, and the records before entering the chain are not within the scope of rule construction. The second is based on legal authenticity. Applying rules such as ‘presumption of business record exceptions’ to Blockchain evidence in various states in the USA shows that judicial practice does not pursue authenticity in the sense of being technically 100% unforgeable for blockchain evidence. This should inspire China’s adherence to the rational truth view on the authenticity of blockchain evidence, that is, the use of blockchain evidence only needs to pursue ‘truth that meets legal standards in specific cases’.⁷⁷ The third is to take the side identification mechanism as the direction. The review and judgment rules of any evidence can be cut from both sides. The former is to provide comprehensive review and judgment elements or standards on the front, and the latter is to provide methods to confirm whether the evidence is true or not. At present, when ordinary judicial personnel are still unable to positively identify the authenticity of blockchain evidence in China, it is a more feasible solution to first build a lateral identification mechanism.

6. Suggestions for blockchain evidence system improvement

6.1 To determine the authenticity of the blockchain evidence, the party claiming that the data has been damaged before uploaded shall bear the burden of proof

Art 69 of the Civil Procedure Law stipulates that ‘the people’s court shall take legal facts and documents notarized through legal procedures as the basis for ascertaining the facts unless there is evidence to the contrary sufficient to overturn the notarized evidence’, which gives the notarized evidence direct legal effect unless there is evidence to the contrary sufficient to overturn it. One of the main reasons why notarized evidence is believed to be authentic is the introduction of a neutral third-party notarization institution to notarize the collection, fixation, and preservation of evidence. Unless there is evidence

76 Caytas Joanna, ‘Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere’ (2017) 3 Columbia Science & Technology Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2988363> accessed 15 April 2023.

77 Pinxin Liu (n 70) 62.

to the contrary, notarized evidence will be considered authentic, but there is no judicial review on whether the generation, storage, and fixation of original data, information, and materials formed before notarization have been damaged, modified, or changed.

The authenticity of electronic evidence requires the authenticity of electronic evidence carrier, electronic data, and electronic evidence content.⁷⁸ Authenticity of electronic evidence carrier is aimed at the storage medium used as electronic evidence carrier and requires the originality, identity of the source, and the identity and integrity of evidence in the process of transfer and circulation, to ensure that the evidence carrier has not been forged, altered, replaced or destroyed; authenticity of electronic data requires the originality, identity of the source and the identity and integrity of the evidence in the process of litigation, to ensure that it has been deleted, modified or added; authenticity of the content of electronic evidence mainly targets at the information contained in the electronic evidence, whether the information can be mutually authenticated with the information contained in other evidence and whether the facts of the case can be accurately proved.

It is known that the blockchain adopts computer technologies such as distributed data storage, de-centralization, encryption algorithm, and consensus mechanism to make the data recorded in the blockchain tamper-proof and irreversible, which means that once authenticated and added to the blockchain, the data will be permanently stored, and there is almost no possibility of human modification, deletion, adjustment or change. Therefore, the data is highly trustworthy and reliable, and the trust problem between users is effectively solved. In this process, the blockchain acts as a neutral third-party organization, with the same function and function as the notarization institution, i.e., to ensure that the data are truly recorded. Since the authenticity of notarized evidence can be directly recognized, similarly, on the premise of no evidence to the contrary to overturn, the authenticity of electronic data stored and authenticated by blockchain technology should also be directly recognized, ie the authenticity of electronic evidence carrier, electronic data, and electronic evidence content. As for whether it has been damaged, modified, or adjusted before being uploaded, and whether it is complete, accurate, and objective, the other party should prove it and produce the evidence on the contrary mentioned above.

6.2 Implementation of access mechanism for third-party evidence storage platform

At present, there is a lack of a unified and practical standard for blockchain electronic evidence. We can consider implementing an access system

78 Fumin Chu, 'Three Levels of Authenticity of Electronic Evidence-Analysis Based on Criminal Procedure' (2018) 4 Chinese Journal of Law 121, 138.

for third-party evidence storage platforms, that is, only blockchain electronic evidence storage carried out by third-party evidence storage platforms with corresponding qualifications can be recognized by judicial authorities. This is similar to notarization institutions and judicial authentication institutions in that all of them need to obtain the corresponding qualifications. At the same time, it is also necessary to actively promote cooperation between the third-party evidence storage platform vs. the judicial services institutions such as courts, arbitration authorities, notarization institutions, and judicial authentication institutions to realize the sharing of resources and data. At present, the arbitration chain of the Guangzhou Arbitration Commission has been set up by WeBank in conjunction with the Guangzhou Arbitration Commission and Hangzhou Yibi Technology based on blockchain technology, and Hangzhou Internet Court has also launched its electronic evidence platform. Such blockchain electronic evidence platform directly built by arbitration institutions or courts undoubtedly greatly improves the credibility and practicability of blockchain electronic evidence. The establishment of the arbitration chain and the successful practice of Hangzhou's Internet electronic evidence platform both illustrate the importance of the access mechanism of the third-party evidence storage platform in promoting and improving the blockchain electronic evidence storage system and enhancing the efficiency and reliability of electronic evidence collection.

6.3 Comprehensive application of network security technology

In the face of the above-mentioned security problems encountered by the blockchain system, it is necessary to comprehensively use network security technologies such as cryptography and mimic defense to improve the security of blockchain from the aspects of algorithms, protocols, passwords, implementations, and systems, etc, in this way to further meet the existing security challenges. For example, institutions or organizations from more countries can be introduced to join the network nodes, nodes with computing power per node of no more than 20% join the entire network and system security experts adopt the best defense technology for blockchain systems.⁷⁹

6.4 Future Development Direction

On the one hand, arbitration has many advantages over litigation. Firstly, the parties involved in arbitration have higher autonomy and can choose the arbitration institution, arbitrator, place of arbitration, arbitration language, arbitration rules, etc. Secondly, arbitration is more efficient than litigation. It takes 6 months for the court to complete the first trial, there may be a second trial after the first trial and still a retrial after the second trial, while arbitration produces

79 Haitao Mei and Jie Liu, 'Industrial Status, Existing Problems and Policy Recommendations of Blockchain' (2016) 11 *Telecommunications Science* 134, 138.

the final decision. Thirdly, arbitration provides better confidentiality. Although court decisions may not be held in public sometimes, such as those involving international secrets and trade secrets, the parties themselves need to apply for it. In contrast, the content of the arbitration agreement is restricted among the parties, arbitrators, and others in a small range. It can be said that these characteristics of arbitration win the favor of many companies and enterprises. According to the above analysis, China's arbitration market is a very large one.⁸⁰ Therefore, the arbitration chain should improve its technology and promote its wider application in the future.

On the other hand, the application of blockchain technology in the judicial field should be faster than that in other industries, because the judicial field itself is a multi-department and multi-institution assistance mechanism, and there is a need for data transmission and case information sharing among the public security bureau, procuratorate, court, and judicial bureau. Although this can be realized with the traditional technology, it is not trustworthy due to the system and mechanism problems and the efficiency is also low. Blockchain technology can be used as assistance. In the future, under the environment of Big Justice, courts and procuratorates may have consortium chains with cross-chain interaction among them. They will be both independent and cooperative with each other. After being approved by the judicial institution, blockchain technology will have very great reference and promotion significance for other industries.

7. Conclusion

The emergence of blockchain electronic evidence storage has brought us many conveniences, which are reflected in both daily life and judicial practice. However, they also bring challenges to the existing state and order. In essence, the emergence of each new technology will impact and change the existing things, and the law is no exception.⁸¹ In this era when new technologies will always present new requirements and challenges to the existing legal system and legal regulations, we should always maintain an open and inclusive attitude, embrace the development of technology, keep up with the pace of the times, constantly revise and improve relevant laws and regulations, and make laws boosters of technological progress. In addition, although the academic circle has already started extensive discussions on the blockchain, most of the documents in the initial stage focus on some simple conceptual issues. Therefore, future research on the blockchain will focus more on the solutions to the problems existing in the blockchain and the application research of the blockchain,

⁸⁰ Yli-Huumo, Jesse and others (n 27) 56.

⁸¹ Jun Zou and Haining Zhang, *Technical Guide for Blockchain* (China Machine Press 2016).

namely the research on putting blockchain technology into practice. With the maturity of blockchain technology and the deepening of people's understanding of blockchain, the problem of blockchain will eventually be solved. When mature blockchain technology is widely used in various fields, the era of 'blockchain+' will follow.

Smart (Legal) Contracts: New Challenge For North Macedonian Legal System

Mirjana Ristovska

Saint Clement of Ohrid University of Bitola, Republic of North Macedonia

ORCID 0000-0002-1766-1919

DOI: 10.54103/milanoup.215.c450

The future is already here - it's just not very evenly distributed.

William Gibson, 1993

Abstract

The global reality of the Fourth Industrial Revolution is evidenced by the adoption of Big Data analytics, Cloud Computing, Blockchain (cryptocurrencies, smart contracts, etc.), and the Internet of Things (smart buildings, artificial neural networks, machine learning, smart cities, etc.) which are becoming integrated into national legislation. As a result, countries must prioritize digitalization to keep pace with Industry 4.0. Smart legal contracts, which serve as a bridge between law and digitalization, are relatively new and challenging development for national legal systems. Although only a few countries have legally regulated smart legal contracts, all national legal systems will inevitably follow suit. This article aims to assess the North Macedonian legal system's existing legislation and determine the optimal approach to integrating smart contracts. Should a new, special law (*lex specialis*) be enacted, or should provisions for smart legal contracts be added to the existing legal framework? The EU's legal tendencies should also be considered to ensure North Macedonian law is harmonized with European Law. The structure of the article unfolds as follows: Introduction; The concept and main characteristics of smart legal contracts, Smart legal contracts concerning the North Macedonian Law on Obligations; Smart legal contracts concerning the North Macedonian Law on electronic commerce; New Law on smart legal contracts or amending the existing legislation in North Macedonia?, and Conclusion remarks. To achieve its goals, this article will employ several research methods, including normative analysis, descriptive and legal research, and applied legal research, comparison, analogy, and case law analyses.

Keywords

Smart Legal Contracts, Traditional Contracts, Digitalization

1. Introduction

The emergence of digital technology has brought about significant changes in contract laws, with the impact of the Internet being one of the most apparent examples. Currently, smart contracts are topic *de jour* in the technology, offering the potential to transform the traditional contracts. Szabo defines smart contracts as a ‘set of promises, specified in digital form, including protocols within which the parties perform on these promises’.¹ Surde envisioned that parties will have the ability to convert specific requirements into a set of computer-readable rules, as well as certain manual comparison between the terms of the contract and the parties’ actual activity could be automated. He points out that this automation could substantially decrease the transaction costs.²

Proponents assert that smart contracts will obviate the need for contract law, revolutionize business arrangements, and restructure property ownership.³ Conversely, skeptics view the blockchain foundation a mere Ponzi scheme.⁴ Some technologists argue that, despite their name, smart contracts have nothing to do with contracts⁵ and some scholar notes that smart contracts are not really ‘smart’ because they cannot (or at least not yet) think or develop, and are not a form of Artificial Intelligence (AI).⁶ Legal futurists tend to present the reduction of legal obligations with the computer code as a positive evolutionary step toward the realization of the rule of law.⁷

Although the impact of the smart contracts on the world is uncertain, they offer tangible advantages and are expected to be widely adopted in the future. The aim of this article is to provide a small contribution towards the integration of modern technologies within the legal field. Instead of hindering the efficient implementation of the advantages of rapid technological advancement, the law should serve as a corrective measure and encouragement. It is crucial to maintain a harmonious relationship between law and technology to effectively

1 Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996) 1 <www.truevalue-metrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf> accessed 30 May 2024.

2 Harry Surden, ‘Computable Contracts’ (2012) 46 University of California Davis 629.

3 Kevin Werbach and Nicolas Cornell, ‘Contracts Ex Machina’ (2017) 67 Duke Journal of Law 313, 317.

4 *ibid.*

5 *ibid.*

6 Maartje Herweijer, ‘Blockchain and the law – Regulation for smart contracts on the way?’ (*Stibbe*, 2019) <<https://www.stibbe.com/>> accessed 30 May 2024.

7 Frank Pasquale, ‘A Rule of Persons, Not Machines: The Limits of Legal Automation’ (2019) 87 The George Washington Law Review 1, 4.

utilize all innovations available to the citizens. In this regard, the protection of human rights and freedoms, as well as the rule of law must remain the imperative. While acknowledging the prevailing view among the legal theorist that smart contracts system will not replace the traditional one, this article advocates for the incorporation and regulation of smart contracts in national legislations, alongside the traditional contracts. This will be able the law to govern and facilitate the growth of smart contract technology. Therefore, the intention of the article is to encourage the acceptance of smart contracts in national and international legislations, including North Macedonian legislation.

2. The concept and main characteristics of smart (legal) contracts

The concept of smart contracts emerged in the legal field only a short time ago, but it has already sparked vastly divergent viewpoints. Accordingly, legal scholars do not share a unanimous opinion concerning the definition of smart (legal) contracts.

Thomas Kulnigg defines legal smart contracts, as the underlying program code that itself qualifies as a legal contract.⁸

Mark Verstraete considers that blockchain-based smart contracts are self-enforcing agreements that ensure performance through technological authority rather than sovereign authority.⁹ Actually, in its article, Verstraete offers a new critique of the optimism about smart contracts and the preference for securing mutual agreements using code, rather than traditional contract law. He challenges the idea that smart contracts can entirely replace traditional contract law. Verstrate point out that unlike previous technology-infused contracts, which relay on a legal system for enforcement, smart contracts aim to be self-executing and autonomous, bypassing or at least being independent of the State's contract law machinery. According to him, this represents a significant departure from earlier attempts to automate contract law trough emerging technologies.¹⁰ Verstrate argues that in a contract system, parties do not require complete trust in each other; rather they rely on trust in the legal system. The foundation of contract law is based on a shared understanding that the legal system will provide a remedy, typically exception damages, if a breach occurs. The crucial difference between the smart contracts and traditional contracts lies in this aspect. Smart contracts, along with other blockchain and internet projects, eliminate

8 Thomas Kulnigg, 'Smart contracts: Too smart for Austrian civil law?' (*Schönherr*, 2018) <www.schoenherr.eu/content/smart-contracts-too-smart-for-austrian-civil-law> accessed 30 May 2024.

9 Mark Verstraete, 'The Stake of Smart Contracts' (2020) 50 *Loyola University Chicago Law Journal* 743, 762.

10 *ibid* 753.

the need for centralized intermediaries. Technologists aim to automate contract law by replacing the legal system with code-based enforcement mechanisms. As a result, smart contract may enable parties to form and enforce the agreements without relying on the state. However, this perspective rests on certain contested assumptions about the role of the state in contract law.¹¹

By Maartje Herweijer, smart contracts are computer protocols that execute pre-determined rules of code: the contractual terms are embedded in software, generally on a blockchain (although smart contracts do not necessarily have to be blockchain-based). Smart contracts cannot be altered retroactively, and will automatically execute or effectuate legal agreements (ie without the cooperation or intervention of the contracting parties or a third party) once they are recorded on a blockchain.¹²

Woebbeking considers that, in a technical sense, smart contracts can be defined as computer protocols that are self-executing. Relying on the abilities of blockchains, they operate autonomously, transparently, and they are basically tamper-resistant and immutable.¹³

De Sevres and others note that a smart contract is created by encoding the terms of a traditional contract and uploading the smart contract to the blockchain. Contractual clauses are automatically executed when pre-programmed conditions are satisfied.¹⁴ Very intriguing view shares Fairfield who defines smart contracts, as automated programs that transfer digital assets within the block-chain upon certain triggering conditions and represent a new and interesting form of organizing contractual activity. In this regard, he points out that if financial transactions can be freed of banks as intermediaries, then contracts can be freed of courts as intermediaries. Finally, he concludes that this will solve a longstanding puzzle and problem of e-commerce: courts' longstanding refusal to enforce contract terms proffered by consumers, ending with the statement that 'if courts will not protect consumers, robots will'.¹⁵

Szczerbowski alerts that two elements of contract law call for attention, regarding the smart contracts: form of contract and contract interpretation. Considering the first element, he contemplates that currently, smart contracts fall into the category of documentary form, which encompasses plain text,

11 *ibid* 754.

12 Herweijer (n 6).

13 Maren K Woebbeking, 'The Impact of Smart Contracts on Traditional Concepts of Contract Law' (2019) 10 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 106, 107.

14 Hossein Kakavand, Nicolette Kost De Sevres, Bart Chilton, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251> accessed 7 July 2024.

15 Joshua A T Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection' (2014) 71(2) *Washington and Lee Law Review Online* 36 <<https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3>> accessed 30 May 2024, 38–39.

emails and text messages (SMS), undervaluing the security provided by blockchain technology. Because of this high level of certainty, usually reserved to written form and electronic form he proposes an addition to the civil law system: blockchain form. Addition of this particular form would enable setting proper presumptions which reflect the secure nature of blockchain transactions – switching the burden of proof to the one who denies the veracity of blockchain, not the one who asserts. Pertaining to the second element, Szczerbowski assesses that interpretation of smart contracts requires a subtler approach as it should depend on the subjective qualities of the parties. For that reason, concludes that it will be most rational to allow courts to establish guidelines for interpreting smart contracts.¹⁶

In its White Paper, the Chamber of Digital Commerce offers two distinct definitions for smart contracts and smart legal contracts. Accordingly, smart contract are ‘computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger’.

On the other hand, smart legal contract are ‘smart contract that articulates and is capable of self-executing, on a legally-enforceable basis, the terms of an agreement between two or more parties’.¹⁷

Based on the definitions and perspectives presented above, it could be inferred that there are two methods for defining smart contracts, which are technical and legal approaches. Therefore it is important to note that not all smart contracts meet the criteria to be classified as legal contracts. As a result, smart contracts refer to contracts that have the capacity to be legally binding and are subject to legal regulations. This article defines smart legal contracts as digital contracts that are self-executed on decentralized blockchain networks, and are legally-enforceable while being automatically fulfilled when predetermined conditions are met.

While various interpretations of the term smart contract exist, there is currently no universally recognized, standardized definition of this term within the legal systems. However, certain legislations have begun incorporating smart contracts into their national laws and regulations, despite the lack of universal definition.

16 Jakub J Szczerbowski, ‘Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation’ (2017) Proceedings of the 12th Annual International Scientific Conference NEW TRENDS 2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3095933> accessed 30 May 2024, 337.

17 Chamber of Digital Commerce, ‘Smart Contracts: Is the Law Ready?’ (Smart Contracts Alliance, 2018) <<https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf>> accessed 30 May 2024, 12.

In its Virtual Financial Assets Act the Republic of Malta has adopted the following definition: ‘smart contract means a form of technology arrangement consisting of (a) a computer protocol; or (b) an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both’.¹⁸

The Republic of Italy also recognizes the legal value of smart contracts. Under the Law No. 12/2019 smart contracts are defined as ‘computer program that works on technologies based on distributed ledgers and which performance automatically binds two or more parties on the basis of the effects previously defined by the parties themselves. Smart contracts fulfill the written form requirement upon prior electronic identification by the parties at hand, through a process the requirements of which are set by the Agency for Digital Italy with guidelines to be adopted within ninety days from the effective date of the entry into force of the decree hereto.’¹⁹

Law on Digital Assets of Republic of Serbia also introduces the term smart contracts: “‘smart contract means a computer program or a computerized protocol based on the distributed ledger technology (DLT) or similar technologies, which is partly or wholly performed by software and which automatically executes, controls or documents legally relevant events and actions according to the terms of a contract already concluded, whereby the contract may be concluded electronically by such program or protocol’.”²⁰

Additionally, in art 37 it is stated that the use of smart contracts in secondary trading in digital assets is allowed and if a digital asset service provider provides services which involve the use of smart contracts, it shall obtain the consent of the digital asset user for the use of smart contracts.

The EU Data Act Proposal accepts the definition as follows: ‘smart contract means a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger’.²¹

Drawing from the definitions mentioned earlier, I can identify the key characteristics that define the smart contracts, which include their ability to self-enforce and operate autonomously, their reliance on software, their conditional structure, and their electronic format.

Self-enforceability is one of the key feathers of smart contracts. A smart contract is a computer program that automatically executes the terms of an

18 Act No XXX of 2018 (ATT Nru XXX 2018) (MT), (2) (2).

19 Italian Decree Law No. 12/2019, art 8-ter <<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2018-12-14;135lvig>>.

20 Law on Digital Assets (Zakon o digitalnoj imovini 2020) (RS), 2 (1) (39).

21 Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), COM(2022) 68 final, 2022/0047 (COD), 2022, Brussels, art 2.

agreement between two or more parties. Once smart contract is concluded, its further execution is no longer dependent on the will of its parties or third party, neither it requires any additional approvals or actions from their side. Computer verifies all the conditions, transfers assets and makes entries in the Blockchain database about such transfers.²² Papantoniou argues that the benefits of smart contracts, including their automaticity and self-enforcement, have been recognized as a way to expand the potential of certain commercial transactions.²³ Additionally, Savelyev notes that smart contracts can function independently without any requirement for a legal system to support them, rendering their existence separate from a broader legal framework. Essentially, smart contracts represent a technological alternative to the whole legal system.²⁴

Smart contracts are essentially software program that run on a blockchain platform.²⁵ Savelyev notes that code is law, and in smart contracts computer code is also contractual terms. Thus, contractual terms are manifested in a computer code, what is not generally prohibited based on the “freedom of contract” principle. He argues that each smart contract by its legal nature is also a computer program in a meaning of IP law. Thus, *smart contract has dual nature in the law: it serves as a “document” governing contractual relations of the parties and it is also object of the IP rights*, representing the valuable object of intellectual activity.²⁶ Pasquale explains that while computer code and human language both enable forms of communication, the affordances offered by each are distinct and, in many respects, mutually exclusive. He points out that code seeks to eliminate the forms of ambiguity and flexibility characteristic of much language, including legal language. Just as quests to replace all standards with rules have failed, so too will most efforts to rewrite legal rules as code.²⁷

Smart contracts include conditions or rules that need to be met for the contract to be executed. Conditions are typically written into the code of the contracts and can include triggers such as the completion of certain actions or the meeting of specific requirements. The computer code is based on statements like ‘if “x” then “y”’.²⁸ Raskin states that performance and enforcement of

22 Alexander Savelyev, ‘Contract law 2.0: “Smart” contracts as the beginning of the end of classic contract law’ (2017) 26(2) Information & Communications Technology Law 116, 126.

23 Alexandros A Papantoniou, ‘Smart contracts in the new era of contract law’ (2020) 1(4) Digital Law Journal 8, 23.

24 Savelyev (n 22) 132.

25 There are various platforms for smart contracts: Ethereum, Hyperledger Fabric, NEM, STELLAR, Waves, and Corda. For more details about their advantages and disadvantages, see: Hamed Taherdoost, ‘Smart Contracts in Blockchain Technology: A Critical Review’ (2023) 14 Information, 117, 8.

26 Savelyev (n 22) 124.

27 Pasquale (n 7) 3.

28 Savelyev (n 22) 126.

a smart contract essentially boils down to conditional statements, which are foundational to computing.²⁹

Smart contracts are created and executed using digital platforms and software, making them electronic in nature. They are written in programming languages and stored on a blockchain, which is a decentralized and distributed digital ledger technology. Sovelyev explains that classic contracts may exist in various forms, e.g. in oral form or in writing and in contrast to that, smart contracts may exist only in electronic form, it is not possible to use any other form of the contract to them (e.g. oral or written hardcopy). He emphasizes that smart contract is limited to the digital world, so only electronic goods/services (exchange of digital goods, transfer of money, etc.) can be the subject of a smart contract.³⁰

3. Smart (legal) contracts in North Macedonian law

In the Republic of North Macedonia, smart contracts currently lack legal recognition as binding instruments, and there is no dedicated legislation in place for their use. Therefore the primary objective in this part of the article is to ascertain whether smart contracts can be covered under the Law on Obligation,³¹ as *lex generalis*, or if there is a need to supplement it. Additionally, an examination will be conducted on the provisions of the Law on Electronic Commerce,³² as *lex specialis* with respect to smart contracts. This analysis will also focus on whether the provisions of this law could extend to smart contracts.

3.1. Smart legal contracts concerning the Law on Obligations

The fundamental concept behind the North Macedonian law regarding contracts is the principle of freedom to regulate obligations. According to art 3 of the Law on Obligations, participants involved in trade have the liberty to regulate the obligations in accordance with the Constitution, the laws, and the good customs. In North Macedonian law, the essential elements of a contract include the mutual assent, the subject of the contract, the legal basis of the contract, the capacity of the contracting parties, and the form of the contract.

29 Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 Georgetown Law Technology Review 304, 312.

30 Savelyev (n 22) 124.

31 Law on Obligations (Закон за облигационите односи 2001) (NMK).

32 Law on Electronic Commerce (Закон за електронска трговија 2007) (NMK).

Table 1. Essential elements of a contract under the Law on Obligations

Mutual assent
Subject of the contract
Legal basis
Capacity of the contracting parties
Form of the contract

Source: Law on Obligations

With regarding the first element, as per Law on Obligations, the contract is deemed to be concluded as soon as the parties involved have agreed on the essential elements of the contract.³³

The assent to enter into a contract may be expressed by words, with the usual signs or other conduct that indicates its existence. Additionally, various modes of communication, such as telephone, fax, internet, and others, can also be used to convey the intention to form a contract. It is essential that the statement of assent be made freely and in a serious manner.³⁴ According to art 23, a contract is established once the offeree communicates his acceptance of the offer to the offeror. The offer, which should include all the essential terms of the contract, can be directed to either a present or absent party.³⁵ As per Law on Obligations, an offer can also be extended through various modes of communications, which is then regarded as an offer between absent parties.³⁶ Acceptance of the offer is deemed to have occurred at the point when the offeror receives a notice from the offeree confirming his acceptance of the offer.³⁷

As the second essential element pertaining to the subject of the contract, the Law on Obligations specifies that the contractual obligation can involve giving, doing, not doing and enduring and that such an obligation must be possible, permitted, and specific or determinable.³⁸ If the subject of the contract is unlawful, undetermined or undeterminable, the contract is rendered nullified.³⁹

As stated in art 43 of the Law on Obligation, each contractual obligation must be founded on a legal basis. The basis is considered legal if it aligns with the Constitution, laws, and good customs and it is presumed that an obligation has a legal basis even it is not explicitly stated. If the basis does not exist or is not permitted, the contract is nullified.⁴⁰

33 art 18 of the Law on Obligations.

34 art 20 of the Law on Obligations.

35 art 24 of the Law on Obligations.

36 art 24-a of the Law on Obligations.

37 art 31 of the Law on Obligations.

38 art 38 of the Law on Obligations.

39 art 39 of the Law on Obligations.

40 art 44 of the Law on Obligations.

The Law on Obligations explicitly requires that the contracting parties must have both legal and business capacity to be eligible for holding rights and responsibilities in a valid contract.

The Law on Obligation specifies that the contract can be established in any form, unless there are legal requirements determining a particular form.⁴¹

Regarding the first essential element of a contract established by the Law on Obligations, I consider that the smart contracts can be recognized as legally enforceable in North Macedonian legislation. This is because the assent to enter into a contract may be expressed by words, with the usual signs or other conduct that indicates its existence. Therefore, it can be inferred that the assent may also be indicated through distributed ledger systems. Expressing assent is significant in this context to be made freely and in a serious manner. In this regard, Werbach and Cornell consider that if a party enters into a smart contract due to fraud or duress, in such a situation, performance may be excused, so the smart contract itself would be valid, but it would be simply not legally enforceable.⁴² Accordingly, creating a smart contract on a distributed ledger and signing it by private key, constitutes a legitimate offer and acceptance under North Macedonian Law on Obligations.

In terms of the second essential element, I also consider that the Law on Obligations encompasses smart contracts. If the legal prerequisite, which is that the subject of the contract must be possible, permitted, and specific or determinable, is not fulfilled, specific issues may arise, especially considering the self-executing nature of smart contracts. In this case, according to the Law, the concluded smart contract will be deemed null and void.

As for the third element, which is the legal basis I believe that it is not applicable to smart contracts. Due to the specific characteristics of smart contracts, I suggest that they should be explicitly introduced by the Law on Obligation.

I am of the opinion that the fourth essential element of contracts may also encompass smart contracts. In terms of applying the forth element to smart contracts, an issue may arise regarding the pseudo-anonymity, where the involved parties may not have information about the other party they are contracting with. In this regard, the Chamber of Digital Commerce considers that the pseudo-anonymity feature in public blockchains can be changed by the design of the blockchain and replaced with identification requirements.⁴³

Concerning the final essential element, this is the form of the contract, I also believe that it is applicable to smart contracts. The phrase 'in any form' encompasses the digital, blockchain, or documentary forms of smart contracts. The Law on Obligations also specifies that the form can be predetermined for specific contracts. If the form of smart contracts is not recognized as a

41 art 59 of the Law on Obligations.

42 Werbach and Cornell (n 3) 369.

43 Chamber of Digital Commerce (n 17) 21.

permissible form, contract with a legally established form cannot be executed as smart contracts.

3.2. Smart legal contracts concerning the Law on Electronic Commerce

A contract that can be completed, transmitted, received, terminated, canceled, accessed, and displayed electronically using electronic, optical, or similar means, including but not limited to Internet transmission, is referred to as an electronic contract under the Law on Electronic Commerce. This contract can be entered into by legal or natural persons either entirely or partly through electronic means.⁴⁴

The contract's form and validity in electronic form are defined in art 10, which permits the contract to be concluded and offer and acceptance to be made electronically. The use of electronic means to make the contract will not render its validity contestable, even if the entire process was concluded through electronic message. Additionally, if the contract requires a person's signature for validity and conclusion, an electronic signature conforming to the electronic signature regulations on an electronic message will fulfill that requirement.⁴⁵ The Law on electronic commerce clearly outlines the types of contracts that cannot be concluded in electronic form, which including the following contracts:

- a. Those falling under the purview of family and inheritance laws;
- b. Those involving the creation or transfer of real estate rights (with the exception of lease right);
- c. Those that require the involvement of courts, notaries, or similar professions as mandated by law, and
- d. Those entered into by individuals for purposes outside their trade, work, or professional engagement, which require a guarantee or additional security.

Art 11 stipulates that, in the absence of any specific provisions in the Law on Electronic Commerce contractual legal relationships resulting from or connected to electronically concluded contracts shall be governed by the Law on Obligations in a subsidiary capacity. According to the Law on Electronic Commerce, an electronic contract is deemed to be concluded when the offeree acknowledges acceptance of a contract's terms through an electronic message. The offer and the acceptance are considered to be received when they are accessible to the parties for whom they are intended.⁴⁶

Given the aforementioned provisions of the Law on Electronic Commerce, I am on the opinion that they are not applicable to smart contracts. Smart contracts differ from the smart contracts in both material and formal aspects.

⁴⁴ art 3 para 1 point 8 of the Law on Electronic Commerce.

⁴⁵ art 10 paras 1, 2, 3, 4 of the Law on Electronic Commerce.

⁴⁶ art 14 of the Law on Electronic Commerce.

Therefore I think this Law should solely pertain to contracts in electronic form and should not be augmented with provisions relating to smart contracts.

3.3. New Law on smart legal contracts

Smart contracts are probably not ‘the mature end of the evolution of electronic agreements’, notwithstanding, they represent a new era of contracting. As seen above, the existing contract law can stand up to some of the challenges posed by smart contracts.⁴⁷

As emphasized in the introduction of the article, I consider that national legal systems should govern smart contracts for two reasons: firstly, smart contracts are a factual occurrence in the digital realm, and their existence should not be disregarded by law. Secondly, it is essential to safeguard the rights and freedoms of citizens and, at the same time, streamline their day-to-day operations. For instance, if smart contracts are not legally governed, and the individual enters into a smart contract despite that, his rights and obligations will be unprotected.

In the light of this, I am of the opinion that the most appropriate approach to incorporating smart contracts into North Macedonian law is by enacting a special Law. The Law should comprise provisions for the legal interpretation of smart contracts; define their scope of application, and explicitly state situations in which smart contracts cannot be applied.

The enactment of the specialized Law for governing smart contracts in the Republic of North Macedonia is essential and should be carried out expeditiously, in line with the obligations for the digitalization of society, as delineated in the National ICT Strategy.⁴⁸

4. Conclusion remarks

Smart contracts offer an opportunity for a novel reinvestigation of contract law, by explicating the reasoning behind contract law rules and by elucidating the precise structure of contract rules by way of formalization in pseudo code.⁴⁹

However, most of the literature concludes that traditional contract law will continue to apply in a smart contract era, and that “smart contracts will never fully replace natural-language law; Nonetheless, many authors also predict that

47 Woebeking (n 13) 112.

48 National ICT Strategy of the Republic of North Macedonia 2023–2027, <<https://shorturl.at/A4OAD>> accessed 30 May 2024.

49 Eric Tjong Tjin Tai, ‘Formalizing Contract Law for Smart Contracts’ (2017) Tilburg Private Law Working Paper Series 6/2017, 8 <<https://ssrn.com/abstract=3038800>> accessed 30 May 2024.

smart contracts can bring clarity, predictability, auditability, and ease of enforcement to contractual relations.⁵⁰

In my opinion, it is necessary to regulate smart contracts through legal norms, due to the many benefits they offer: increased speed, efficiency, cost effectiveness, highly secure, greater accuracy, clear communication, paper free and so on.⁵¹ This does not imply that ‘the law will become the subdivision of commuter science’.⁵²

The main goal of the article was to assess the North Macedonian legal system’s existing legislation and determine the optimal approach to integrating smart contracts. So, as previously stated in the context of North Macedonian Law, I consider that the following steps should be taken: firstly, the Law on Obligation should be amended to include smart contracts as a distinct type of contract, and secondly a special Law should be enacted to define and regulate all relevant details and specificities related to smart contracts.

I strongly believe that smart contracts as created by technology, will not be the ‘problem’ for the law.

50 J Dax Hansen, Laurie Rosini, Carla RReyes, ‘More Legal Aspects of Smart Contract Applications’ (2018) White paper, Perkins Coie 1, 6, <<https://www.perkinscoie.com/images/content/1/9/v3/199672/2018-More-Legal-Aspects-of-Smart-Contract-Applications-White-Pa.pdf>> accessed 07 July 2024.

51 Pete Peranzo, ‘Smart Contracts in Real Estate: Benefits, Use Cases, and Examples’ (*Imagination*, 2023) <<https://imagination.net/blog/smart-contracts-in-real-estate/>> accessed 30 May 2024.

52 Pasquale (n 7) 2.

Banking and Financial Digital Platforms: Conflict of Laws Issues from a European Perspective

*Silvia Favalli **

University of Milan, Italy

ORCID 0000-0002-8579-6284

DOI: 10.54103/milanoup.215.c451

Abstract

Advances in technologies, such as enhanced computing power, cryptography and artificial intelligence, are transforming the way banking and financial services are provided. On the one hand, disruptive disintermediation-enabling technology, belonging to alternative finance forms, is challenging traditional banking intermediaries' role. On the other hand, new intermediaries, whose activities have not traditionally encompassed finance, such as social media companies, are being drawn into the financial industry. Moreover, increased internet speed and easier mobile access are giving rise to rapid growth in the use of banking and financial digital platforms, in particular among consumers, start-ups, SMEs and social enterprises. This trend is also expected to accelerate, as digital platforms reduce costs, facilitate access to financial products and services, and enhance cross-border operations. However, as a consequence, new private international law problems are emerging along with the widespread use of digital platforms. Against this background, this paper, which is informed by a doctrinal legal methodology, addresses the emerging conflict of laws issues European users of banking and financial digital platforms face. For this purpose, it will first set the scene of the relevant EU legal framework in relation to banking and financial digital platforms, categorized, on the basis of the function they perform, as follows: (i) lending and financing fintech platforms, including balance-sheet lending and crowdfunding platforms; (ii) robo advice and algorithmic trading platforms; (iii) digital payment services and e-money; (iv) financial services related to crypto assets. On the basis of the analysis provided, it will finally focus

* This research was supported by the project 'DigIFin: La digitalizzazione delle transazioni finanziarie come fattore di internazionalizzazione delle PMI attraverso nuovi strumenti di accesso al credito', financed by the Italian Minister of University and Research under the National Operational Programme on Research and Innovation (PON) 2014-2020.

on the forum and applicable law issues faced by European users of banking and financial digital platforms.

Keywords

Banking and financial digital platforms; Brussels I bis Regulation; Rome I Regulation; Rome II Regulation

1. Introduction

Increased internet speed and easier mobile access are giving rise to rapid growth in the use of banking and financing digital platforms, particularly among consumers, start-ups and SMEs. This trend is also expected to accelerate, as fintech platforms¹ reduce costs, facilitate access to financial products and services, and enhance cross-border operations.²

In particular, the use of banking and financing digital platforms is widespread both in traditional banking and in alternative finance.³ On the one hand, enhanced computing power, cryptography and artificial intelligence are giving rise to new opportunities for the development of the traditional financial industry, which benefits from such advances in technologies. On the other hand, disruptive disintermediation-enabling technology, belonging to alternative finance forms, is challenging traditional banking intermediaries' role. New intermediaries, whose activities have not traditionally encompassed finance, are being drawn into the financial industry. For instance, common payment platforms have been developed not only by credit institutes but also by major social media companies (so-called Big tech).⁴

In this light, in 2020 the EU adopted a digital finance package, with the ambition to boost Europe's competitiveness and innovation in the financial sector while embracing the digital transition. The package includes a digital finance

1 For the purposes of this paper, the definition of fintech as "technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services" provided by the Financial Stability Board (FSB) will be adopted See FSB, 'Financial stability implications from fintech: supervisory and regulatory issues that merit authorities' attention' (27 June 2017) 1.

2 J Ehrentraud and others 'Policy responses to fintech: a crosscountry overview' (2020) Financial Stability Institute FSI Insights on policy implementation No 23, 11 <<https://www.bis.org/fsi/publ/insights23.pdf>> accessed 30 May 2024.

3 For a definition of alternative finance, see T Ziegler and others, 'The 2nd Global Alternative Finance Market Benchmarking Report' (Cambridge Centre for Alternative Finance 2021), 30 <<https://www.jbs.cam.ac.uk/wp-content/uploads/2021/06/ccaf-2021-06-report-2nd-global-alternative-finance-benchmarking-study-report.pdf>> accessed 30 May 2024.

4 K Croxson and others, 'Platform-based business models and financial inclusion' Bank for International Settlements BIS Working Papers No 986 2022, 23 <<https://www.bis.org/publ/work986.pdf>> accessed 30 May 2024.

strategy,⁵ legislative proposals on crypto-assets (MiCA Regulation)⁶ and digital resilience (DORA),⁷ and a renewed retail payments strategy.⁸ Moreover, in the framework of the Capital Markets Union Action Plan⁹ and of the Fintech Action Plan,¹⁰ the Commission adopted the so-called crowdfunding regulation¹¹ to facilitate the exercise of the freedom to provide and receive such services cross-border in the internal market.

The digitisation of the services offered facilitates the involvement of market players from different jurisdictions, resulting in cross-border banking and financial services among European users. This represents both an opportunity for the EU economy and a new challenge for the EU private international law legal framework, as it means dealing with the peculiarities of the application of conflict of laws rules in two different areas of law, respectively, the digital arena and finance. On the one hand, the internet, which ignores geographical borders, represents a unique challenge for private international law under several profiles,¹² spanning from the protection of personality and intellectual property rights to the prevention of unfair competition, the regulation of parties' agreements, the protection of weaker contract parties and the localisation of the place of damage. On the other hand, the area of finance necessitates some exceptions from the application of the common rules of EU private international law.¹³ Against this background, this contribution addresses emerging conflict of laws issues from a European perspective.¹⁴

After this introduction, section 2 sets the scene of the relevant EU legal framework in relation to fintech platforms, categorized on the basis of the

-
- 5 Commission, 'Communication on a Digital Finance Strategy for the EU' [2020] COM (2020) 591 final.
 - 6 Regulation 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150 (hereafter, MiCA Regulation).
 - 7 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L 333 (hereinafter, DORA).
 - 8 Commission, 'Communication on a Retail Payments Strategy for the EU Brussels' COM (2020) 592 final.
 - 9 Commission, 'Action Plan on Building a Capital Markets Union Brussels' (Communication) COM (2015) 468 final.
 - 10 Commission, 'Fintech Action plan: For a more competitive and innovative European financial sector' (Communication) COM (2018) 109 final.
 - 11 Regulation (EU) 2020/1503 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 [2020] OJ 2 347/1.
 - 12 D Jerker and B Svantesson, *Private International Law and the Internet* (3rd edn, Wolters Kluwer 2016) 51; P De Miguel Asensio, *Conflict of Laws and the Internet* (Edward Elgar 2020) 409.
 - 13 See M Lehmann, 'Private international law and finance: nothing special?' [2018] NIPR 3.
 - 14 Private international law and conflict of laws are used synonymously in this contribution.

function they perform. sections 3 and 4 focus, respectively, on the forum and applicable law issues. Section 5 completes the analysis addressing choice-of-court and choice-of-law agreements concluded by the parties. To this end, the provisions of Regulation (EU) No 1215/2012 (Brussels I-bis Regulation),¹⁵ the 2007 Lugano Convention¹⁶ and the Hague Convention of 2005¹⁷ on forum law, as well as Regulations (EU) No 593/2008 (Rome I Regulation)¹⁸ and Regulation (EU) No 864/2007 (Rome II Regulation)¹⁹ on applicable law are taken into consideration. Section 6 concludes.

2. Defining banking and financing digital platforms

Digital platforms are a widespread phenomenon in the EU economy, representing an unprecedented opportunity for innovation and growth, particularly for start-ups and SMEs. They cover a wide-ranging set of activities, including ‘online advertising platforms, marketplaces, search engines, social media and creative content outlets, application distribution platforms, communications services, payment systems, and platforms for the collaborative economy’.²⁰

However, given the breadth of use and differing models, there is no single definition of an online or digital platform. Moreover, in the context of a public consultation on the regulatory environment for platforms promoted by the Commission in 2015,²¹ it emerged that the majority of the participating

15 Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L 351 (hereinafter, Brussels I-bis).

16 Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2007] OJ L 339 (hereinafter, 2007 Lugano Convention).

17 Hague Convention of 30 June 2005 on Choice-of-court Agreements (hereinafter, 2005 Hague Convention).

18 Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177.

19 Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L 199.

20 Commission, ‘Online Platforms and the Digital Single Market Opportunities and Challenges for Europe’ (Communication) COM (2016) 288 final, 2.

21 Commission, ‘Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy’ (Commission’s public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, opening 24 September 2015) <<https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud-computing>> accessed 6 March 2023. In the consultation, the Commission provides an attempted definition of online platform, which reads as follows: ‘an undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups. Certain platforms also qualify as Intermediary service providers’. For an in-depth analysis of the attempted definition provided by the Commission

stakeholders contested the opportunity to provide a possible legal definition of online platforms. In particular, major concerns refer to the feasibility of a ‘one-size-fits-all’ definition, as it is unlikely to be ‘future-proof’ and might overlap with other notions, such as those of online intermediaries and information society service providers.²² In this vein, it is contended that a generic notion of online platforms is too vague to provide a framework that would be fit for the purpose and ensure legal certainty.²³ Along this line, every EU legislative act regulating digital platforms subsequently adopted provides an autonomous definition, relevant to the particular subject matter.²⁴

Such an approach has been adopted also in the fintech area, where different definitions and categorisations of digital and financial platforms have been developed to date.²⁵ Moreover, the taxonomy used within the fintech space gives

in the context of the consultation, see also House of Lords, ‘Online Platforms and the Digital Single Market’ (10th Report of Session 2015–16) 22.

- 22 Commission, ‘Synopsis report on the public consultation on the regulatory environment for platforms, online intermediaries and the collaborative economy’ (Commission’s public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, opening 24 September 2015) <<https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud-computing>> accessed 6 March 2023, 6.
- 23 Oxera Consulting LLP, ‘Benefits of online platforms’ (2015), 16 <<https://www.oxera.com/wp-content/uploads/2018/07/The-benefits-of-online-platforms-main-findings-October-2015.pdf.pdf>> accessed 30 May 2024.
- 24 See art 2 lett. *i* of Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277; art 2 n 2 of Regulation (EU) 2022/1925 (Digital Market Act); Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L 265; art 1 n 1 of the Proposal for a Directive on improving working conditions in platform work COM (2021) 762. Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186, which focuses on one of the different services offered by digital platforms, ie online intermediation services, does not provide a definition of platform. However, recital n 49 refers to the key role played by the group of experts for the Observatory on the Online Platform Economy, established in accordance with the Commission Decision C(2018)2393, in informing the evaluation of this Regulation by the Commission. The Observatory defines online platforms as ‘online spaces where users are brought together by a platform operator in order to facilitate an interaction (exchange of information, a commercial transaction, etc.)’. See PPMI, Open Evidence, Rand Europe, German Economic Institute (IW), ‘Study on Support to the Observatory for the Online Platform Economy’ (Study implemented for the European Commission 3 May 2021) 29.
- 25 Among many, see OICV-IOSCO, ‘Research Report on Financial Technologies (Fintech)’ (February 2017) <<https://www.iosco.org/library/pubdocs/pdf/IOSCPD554.pdf>> accessed 30 May 2024; P Cipollone, ‘Conference on Digital Platforms and Global Law’ (Banca d’Italia 29 April 2022) <https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2022/en_CIPOLLONE_29_aprile_2022.pdf?language_id=1> accessed 30 May 2024 <<https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2022/>

rise to uncertainty, as often contributors use different terms for the same activity or the same term for different ones.²⁶

Against this background, for the purposes of this contribution fintech platforms are broadly considered as technical infrastructures that enable users to establish banking and financial legal relationships with each other. More precisely, banking and financial platforms are categorized, on the basis of the function they perform, as: (i) lending and financing fintech platforms, including balance-sheet lending and crowdfunding platforms; (ii) robo-advice and algorithmic trading platforms; (iii) digital payment services and e-money and (iv) financial services related to crypto assets.²⁷

2.1. Lending and financing fintech platforms

Lending and financing fintech platforms act as intermediaries for typical activities of the banking and financial sector, such as granting loans or placing financial instruments. It is possible to distinguish between balance-sheet lending and crowdfunding platforms.

Balance-sheet lending platforms assume credit risk by keeping originated loans on their balance sheet, as they perform credit activity using their own balance sheet in the ordinary course of business to intermediate borrowers and lenders.²⁸ Such platforms, which are widespread in the US, use intermediaries having the necessary authorisations to perform credit activity in the EU.²⁹ This is the case, for example, with the US platforms Kabbage and PayPal Credit, which use the intermediation services of the banking group ING and the Luxembourg-based credit institution PayPal (Europe) S.à.r.l. et Cie S.C.A., respectively.

Crowdfunding (or crowdfinancing) platforms are publicly accessible internet-based information systems that match the business funding interests of investors and project owners through a crowdfunding platform.³⁰ They are divided into investment-based or lending-based on the basis of the financial activity they perform. More precisely, in investment-based crowdfunding, investors

CIPOLLONE_29_aprile_2022.pdf; EBA, 'Report on the use of digital platforms in the EU banking and payments sector' (September 2021) EBA/Rep/2021/26.

26 J Ehrentraud and others, 'Policy responses to fintech' (n 2) 6.

27 Such a categorisation lays its foundations on the theorisation of the 'fintech tree' elaborated in J Ehrentraud and others (n 2). However, this contribution will not consider the insurtech sector, mentioned in the 'fintech tree'. Notwithstanding their close relationship, fintech and insurtech lay their foundations on different legal frameworks, which deserves separate legal analysis.

28 *ibid* 8.

29 Art 8 of Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L 176.

30 Art 2(1)(a) of Regulation (UE) 2020/1503.

provide private companies with equity (equity crowdfunding) or debt securities (debt-based crowdfunding). In lending-based crowdfunding, platforms facilitate the credit activity performed among investors and project owners. These include invoice trading and peer-to-peer crowdfunding platforms.

Crowdfunding services have a tripartite structure, involving project owners, investors and crowdfunding service providers, where each of the actors is in a bilateral relationship with the other two. The recently adopted Regulation (EU) 2020/1503 sets out common rules for organising, authorising and supervising crowdfunding service providers that are established in the EU. It applies in the Member States from 10 November 2023.

2.2. Robo-advisors and algorithmic trading platforms

Robo-advisors and algorithmic trading platforms rely on automated or semi-automated systems (algorithm-based tools) with the aim to offer investment services with no or limited human intervention.³¹ While robo-advisors provide investment advice, algorithmic trading platforms make transaction decisions in the financial markets.³²

The MiFID II package requires the implementation of appropriate controls for investment services provided through an automated or semi-automated system activity to mitigate the risks correlated. art 54 and recital n 86 of Regulation (EU) 2017/565,³³ implementing art 25 of Directive 2014/65/EU,³⁴ set out that, where investment advice or portfolio management services are provided through an automated or semi-automated system, the responsibility to undertake the suitability assessment shall not be reduced using an electronic system in making the personal recommendation or decision to trade.

Moreover, art 17 of Directive 2014/65/EU introduces closer regulation and monitoring of algorithmic trading,³⁵ imposing new and detailed requirements on algorithmic traders and trading venues. In this vein, it constitutes an exception to the principle of technology neutrality generally pursued in financial

31 P Maume, *Robo-advisors. How do they fit in the existing EU regulatory framework, in particular with regard to investor protection?* (Publication for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament 2021) 19.

32 European Supervisory Authorities (ESAs), 'Report on automation in financial advice' (JC SC CP FI/2016/24 2016) 12-15.

33 Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive [2007] OJ L 87/1.

34 Directive 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L 173/349.

35 Art 4(1) n 39 of Directive 2014/65/EU (n 34).

regulation.³⁶ Similarly, also high-frequency algorithmic trading, which is a specific subset of algorithmic trading where the trading system analyses data at high speed and sends large numbers of orders within a very short time in response to that analysis, is subject to particular regulatory scrutiny under MiFID II.

2.3. Digital payment and e-money service providers

Digital payment service providers use technology to facilitate payment transactions without the use of physical money. Instead of currency, some providers use e-money, referred to as electronically stored monetary value which represents a fixed value claim on its issuer for the purpose of making payment transactions.³⁷

There is a broad spectrum of payment platforms, which operate at different stages of the payment chain and engage in various payment-related activities.³⁸ Payment services are provided by both credit institutions and alternative intermediaries. The platforms developed by major social media companies, such as Amazon, Apple, Facebook and Google (so-called Big tech), reached an impressive diffusion worldwide.³⁹ Amazon Pay is an electronic money institution that issues e-money to make payments, while Apple Pay, Meta Pay (which replaced Facebook Pay) and Google Pay are e-wallets that store payment information and allow users to securely make a purchase.

The Payment Services Directive (PSD2)⁴⁰ sets out common rules concerning the granting of authorisation to provide and execute payment services throughout the Union. According to art 11 PSD2, the authorisation delivered by the competent authorities of a Member State allows the payment institution concerned to provide the payment services that are covered by the authorisation throughout the EU. E-money service providers must comply also with the requirements of the Electronic Money Directive (EMD2), which lays down the rules for the pursuit of the activity of issuing e-money. For example, the

36 F Annunziata, 'I processi di mercato automatizzati e il trading algoritmico', in M Cian, C Sandei, *Diritto del Fintech* (Cedam 2020) 402.

37 Art 2 n 2 of Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L 267.

38 For an attempt to categorize these platforms see J Ehrentraud and others 'Fintech and payments: regulating digital payment services and e-money' (2020) FSI Insights on policy implementation No 33, 10 <https://www.bis.org/fsi/publ/insights33.pdf> accessed 30 May 2024; J Ehrentraud and others (n 2) 22.

39 G7 Working Group on Stablecoins 'Investigating the impact of global stablecoins' (2019) Committee on Payment and Market Infrastructures (CPMI), 28 <https://www.bis.org/cpmi/publ/d187.pdf> accessed 30 May 2024.

40 Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35.

US provider PayPal can pursue its activity in the EU using as an intermediary PayPal (Europe) S.à r.l.et Cie, S.C.A., a Luxembourg-based credit institution.

2.4. Financial services related to crypto assets

Crypto assets, defined as digital representations of value or rights which may be transferred and stored electronically using distributed ledger technology (DLT),⁴¹ can be used to provide different financial services. Likewise, in the operations of initial public offerings of shares of private companies, crypto assets can be offered to the public to raise capital. This operation, called an initial coin offering (ICO), consists of the generation of a certain amount of a new token specifically for the funded business project and their offering in exchange for a certain amount of cryptocurrency or legal tender.⁴²

The rapid spread worldwide of crypto assets in finance has led to the development of numerous international initiatives aimed at integrating these tools into legislative frameworks regarding their regulation, supervision and oversight.⁴³ Along the same line, in 2020 the EU launched two proposals of regulations relevant to the harmonization of rules regarding financial services related to crypto assets. The MiCA Regulation⁴⁴ sets out uniform requirements for the offering and placing on the market of crypto assets. The DORA (Digital Operational Resilience Act)⁴⁵ establishes an oversight framework for critical ICT third-party providers, including crypto assets providers. The Commission also

41 Art 3(1) n 2 MiCA Regulation

42 P Ortolani, 'Civil and Commercial Jurisdiction in Crowdfunding-Related Litigation', in P Ortolani, M Luoisse (eds), *The EU Crowdfunding Regulation* (OUP 2021) 120. Initially, the term ICOs was exclusively associated with the issuance of cryptocurrencies (eg bitcoin or ether), whereas it is currently used to identify any token offerings. Different terms have emerged depending on the type of crypto assets offered: UTOs (utility token offerings), STOs (security token offerings), which in turn can be distinguished into ETOs, if it concerns the offering of venture capital (equity token offerings) and ICCOs, if it concerns the offering of tokens convertible into shares (initial convertible coin offerings).

43 FSB, 'Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations' (2020) <<https://www.fsb.org/wp-content/uploads/P131020-3.pdf>> accessed 30 May 2024; BCBS, 'Prudential treatment of cryptoasset exposures' (Consultative Document 2021; CPMI-IOSCO, 'Prudential treatment of cryptoasset exposures' (2021) <<https://www.bis.org/bcbs/publ/d545.pdf>> accessed 30 May 2024; IOSCO, IOSCO decentralized finance report (March 2020) OR01/2022; OECD, 'Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard' (2022).

44 Regulation 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150.

45 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L 333.

launched the Anti-money laundering and countering the financing of terrorism legislative package,⁴⁶ which includes legislative initiatives recognising crypto assets service providers among the entities required to adopt specific measures to prevent money laundering and terrorist financing.⁴⁷

To date, there is no common taxonomy of crypto assets. However, based on the function they perform, it is possible to identify specific subcategories of crypto assets, namely payment or currency tokens (cryptocurrency), utility tokens, investment or security tokens.⁴⁸ Payment or currency tokens are digital representations of value that are not issued or guaranteed by a central bank or public authority, are not necessarily attached to a fiat currency but are used by natural or legal persons as means of exchange and can be transferred, stored, or traded electronically.⁴⁹ According to the Court of Justice (CJEU), they are ‘a contractual means of payment’;⁵⁰ unlike e-money, for cryptocurrencies, the funds are not expressed in traditional accounting units, such as in euro, but in virtual accounting units, such as the bitcoin. Stablecoins are cryptocurrencies which sought a stable value.⁵¹ Under the MiCA Regulation, stablecoins are distinguished between asset-referenced token, which aims at maintaining a stable value by referencing several currencies that are legal tender, one or several commodities, one or several crypto-assets, or a basket of such assets, and e-money-token, which are purports to maintain a stable value by referring to the value of a fiat currency that is legal tender. Utility tokens have non-financial purposes, as they are intended to provide digital access to a good or service, available on DLT, and that is only accepted by the issuer of that token. Unlike cryptocurrency and utility tokens, security tokens are excluded from the scope of the MiCA Regulation.⁵² As digital forms of traditional financial instruments such as stocks, bonds, or other securitized assets, they are the only form of crypto

46 Commission, ‘Towards better implementation of the EU’s anti-money laundering and countering the financing of terrorism framework’ (Communication) COM (2019) 360 final.

47 Regulation 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 [2023] OJ L 150.

48 EBA, ‘Report with advice for the European Commission on crypto-assets’ (EBA Report 2019) 7.

49 EBA, ‘Opinion on virtual currencies’ (2014) EBA/Op/2014/08. More recently, see art 3 n 18 of Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43.

50 Case C–264/14 *Skatteverket v David Hedqvist* [2015] ECLI:EU:C:2015:718, para. 42.

51 D Arner, R Auer, J Frost, ‘Stablecoins: risks, potential and regulation’ (2020) BIS Working Papers No 905, 6; FSB, ‘Addressing the regulatory, supervisory and oversight challenges raised by “global stablecoin” arrangements: Consultative Document’ (14 April 2020), 8 <https://www.fsb.org/wp-content/uploads/P140420-1.pdf> accessed 30 May 2024.

52 Art 2(2)(a) MiCA Regulation.

assets capable of being classified as financial instruments under art 4(1) n 15 of MiFID II.

3. Forum law issues

Along with increasing cross-border provision of banking and financial services among European users, fintech platforms are also facilitating the emergence of new litigation scenarios involving forum law issues. In particular, this contribution focuses on the most common hypothesis involving a European user of banking and financial platforms, where the investor (payee in payment services) brings a claim against the service provider.

Crowdfunding and ICOs (initial coin offerings) platforms are exceptional, as they have a tripartite structure. Therefore, in the analysis below, some clarifications will be provided about such platforms, where two scenarios will be considered. In the first one, the investor brings a claim against the service provider. In the second one, the investor brings a claim against the project owner of the crowdfunding service or the issuer of the ICOs.

When the service provider is domiciled in a Member State, the provisions of the Brussels I-bis Regulation are applicable. The domicile is identified, in compliance with art 63, at the place where it has its statutory seat, central administration, or principal place of business.

In case the defendant is not domiciled in a Member State, the jurisdiction is not determined by the provisions of Brussels I-bis Regulation, but by the law of the courts of that Member State.⁵³ However, when the investor is a consumer, Brussels I-bis Regulation applies regardless of whether the defendant is domiciled in a third State.⁵⁴ When a European user brings a claim against a service provider domiciled in a State party of the 2007 Lugano Convention,⁵⁵ namely Norway, Iceland and Switzerland, the 2007 Lugano Convention applies.⁵⁶ Its rules are mostly similar to those provided by Brussels I-bis Regulation.

53 Art 6 Brussels I-bis Regulation (EU) 2020/1503 requires that crowdfunding services can only be provided by legal entities established in the EU (art 3). Accordingly, this Regulation does not apply to platforms domiciled in a third State.

54 Art 18(1) Brussels I-bis

55 2007 Lugano Convention (n 16).

56 The convention entered into force on 1 January 2010 in the EU and Norway, while on 1 January 2011 in Switzerland and on 1 May 2011 in Iceland. The convention was also signed by the Kingdom of Denmark. However, Denmark has by letter of 20 December 2012 notified the Commission of its decision to implement the contents of Regulation Brussels I-bis. This means that the provisions of Regulation Brussels I-bis will be applied to relations between the Union and Denmark. See the Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2013] OJ L 79/4.

Art 4 Brussels I-bis establishes, as a general rule, the jurisdiction of the courts of the defendant's place of domicile. However, art 7 gives the claimant the option to sue him before the courts of a different Member State in special hypotheses. The relevant ones for the purposes of this contribution refer to contractual matters, torts, and disputes arising from the operations of a branch. Moreover, when the investor can be qualified as a consumer, as he is automatically considered the weaker party of the dispute, according to art 17, a partially different regime applies. Further analysis of contractual, consumer and tort jurisdiction will be provided in the subsections below.

Moreover, to safeguard the jurisdiction of the courts of the Member States in situations where they have exclusive jurisdiction, certain rules of jurisdiction should apply regardless of the domicile of the parties. In this line, 'in proceedings which have as their object the validity of the constitution, the nullity or the dissolution of companies or other legal persons or associations of natural or legal persons, or the validity of the decisions of their organs' the courts of the Member State of incorporation (*lex societatis*) has exclusive jurisdiction according to art 24 No 2. Such a hypothesis may occur in equity-based crowdfunding and ETOs (equity token offerings) platforms, which both concern the offering of venture capital.

3.1. Contractual jurisdiction

In matters relating to a contract,⁵⁷ Brussels I-bis Regulation gives the investor the option to sue the service provider before the courts of the place of performance of the obligation in question, as long as this is located in a Member State. Art 7(1)(b) Brussels I-bis clarifies that in the cases of the sale of goods and of the provision of services the place of performance is in a Member State where, under the contract, respectively, the goods were delivered, and the services were provided. This special forum often coincides with the domicile of the investor, who will therefore have an interest in bringing proceedings before the court thus identified.

Regarding the first hypothesis, it is crystal clear that financial transactions which involve the transfer of tangible goods in exchange for units of a cryptocurrency might be classified as a contract for the sale of goods under art 7(1)(b) Brussels I-bis. To contrast, it is questionable whether a contract requiring the transfer of tangible goods in exchange for units of a cryptocurrency fits in the

⁵⁷ Contractual matters cover situations in which there is an obligation freely assumed by one party towards another. Among many, see Case C-26/91, *Handte v TMCs* [1992] ECR I-3967; Case C-548/12, *Marc Brogitter v Fabrication de Montres Normandes EURL, Karsten Fräßdorf* [2014] ECLI:EU:C:2014:148, paras 23–25; Case C-196/15, *Granarolo SpA v Ambrosi Emmi France SA* [2016] ECLI:EU:C:2016:559, paras 21–27; Case C-59/19, *Wikingerbhof GmbH & Co. KG v Booking.com BV* [2020] ECLI:EU:C:2020:950, para 32.

same qualification, as, in the absence of any judicial decision confirming this point, there remains some doubt about such a classification.⁵⁸

The second hypothesis of art 7(1)(b) Brussels I-bis, regarding the provision of services, embraces numerous scenarios. In general, it might refer to the duties of information to the client that falls on the service provider, according to the investor protection discipline of different legal instruments. Art 19 of Regulation 2020/1503 requires that crowdfunding platforms provide a series of information to investors, while art 20 of the same regulation imposes the annual disclosure of the default rates of the crowdfunding projects offered on their crowdfunding platform.⁵⁹ Likewise, art 24 of MiFID II provides similar obligations to investment advisors, including robo-advisors. Art 52 of PSD2 lays down a long list of information and conditions which should be provided by the payment service provider to the user. Moreover, art 89 PSD2 clarifies that the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.

Finally, according to art 7(5) Brussels, when the dispute arises out of the operations of a branch, agency or other establishments of the service provider, jurisdiction lies also in the courts for the place where the branch, agency or other establishment is situated.

3.2. Consumer jurisdiction

Brussels I-bis Regulation lays down rules of jurisdiction more favourable to the interests of consumers, who are considered weaker parties in the dispute. In this vein, pursuant to art 18(1), a consumer may bring proceedings either in the courts of the Member State in which the service provider is domiciled or,

58 A Dickinson, 'Cryptocurrencies and the Conflict of Laws', in D Fox, S Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019) 98. On the one hand, to support the qualification as contract for the sale of goods under art 7(1)(b) Brussels I-bis, it is possible to infer that the CJEU case law adopted a flexible approach focussing on the contract's characteristic performance rather than the promised counter-performance (Case C-381/-08, *Car Trim GmbH v KeySafety Systems Srl* [2010] ECR I-1255). This is also in line with the CJEU case law on VAT legislation affirming that 'the 'bitcoin' virtual currency has no purpose other than to be a means of payment and that it is accepted for that purpose by certain operators': see *Skatteverket v David Hedqvist* (n 50). On the other hand, to contrast such a qualification, it is also worth mentioning that the same CJEU case law affirmed that the characterization of a transaction for VAT purposes is not necessarily to be carried across to the EU private international law instruments (Case C-533/07, *Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindbors* [2009] ECR I-3327, paras 37-40).

59 The mere circumstance that a certain Member State has been indicated by the crowdfunding service provider for the purposes of art 18(1)(a) of Regulation (EU) 2020/1503 is not sufficient to establish jurisdiction in the courts of that Member State, in the absence of any concrete territorial link between that State and the facts of the case. See P Ortolani (n 42) 330.

regardless of the defendant's domicile, in the courts for the place where the consumer is domiciled.

The investor can be qualified as a consumer if three conditions are met. First, the investor is acting in a context which can be regarded as being outside his trade or profession. Second, the contract between a consumer and a professional has actually been concluded. Third, in compliance with art 17, such a contract “has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities”.⁶⁰

Concerning the first condition, only natural persons acting in a context which can be regarded as being outside their trade or profession can qualify as consumers. Therefore, investors who are legal persons, such as SMEs or start-ups, are automatically excluded.

In addition, rules of jurisdiction referring to consumers do not apply to equity-based crowdfunding and ETOs (equity token offerings) platforms, whereas, as a matter of principle shareholders are not consumers.⁶¹ To contrast, such rules may apply to investors of, for instance, debt-based crowdfunding, ICOs (initial coin offerings) or lending-based crowdfunding platforms, as long as holders of securities other than shares may qualify as consumers.⁶²

Moreover, the distinction between the term ‘consumer’ under Brussels I-bis Regulation and ‘retail client’ under MiFID II needs clarification. In *Petruchová*,⁶³ the Court of Justice specified that those two concepts pursue different objectives. The classification as retail client seeks to protect an investor, in particular as regards the scope of the information that the investment firm is required to provide to him, while the qualification as a consumer affords protection when the court competent to rule on a dispute is determined. Therefore, a person's status as a retail client within the meaning of MiFID II is irrelevant for classifying him as a consumer within the meaning of art 17(1) Brussels I-bis. Analogous reasoning applies also to the relationship between the concept of ‘consumers’ under Brussels I-bis Regulation and ‘non-sophisticated investors’ of crowdfunding platforms introduced by Regulation (EU) 2020/1503, as the definition of non-sophisticated investors builds upon the notion of retail clients established in MiFID II.⁶⁴ Therefore, the notion of ‘non-sophisticated’

60 Among many, see Case C-375/13 *Harald Kolassa v Barclays Bank plc* [2015] ECLI:EU:C:2015:37, para 23.

61 M Gargantini, ‘Prospectus Liability: Competent Courts of Jurisdiction and Applicable Law’, in D Busch, G Ferrarini, JP Franx (eds), *Prospectus Regulation and Prospectus Liability* (OUP 2020) 459–460.

62 *ibid.*

63 Case C-208/18, 3 *Jana Petruchová v FIBO Group Holdings Limited* [2019] ECLI:EU:C:2019:825.

64 Recital n 42 of Regulation (EU) 2020/1503.

investor under Regulation is essentially unrelated to the notion of ‘consumer’ under Brussels I-bis Regulation.⁶⁵

Regarding the second condition, since the dispute should concern a contract actually concluded between the parties, subsequent acquisitions of the same financial instrument are excluded. Therefore, financial transactions established in the primary market between issuer and underwriter fall under this hypothesis, while contracts concluded between issuer and subsequent investors intervened in the secondary market are not relevant. Moreover, contracts concluded in the secondary market between financial intermediary and investor may fall within the scope of art 17.⁶⁶ Moreover, it implies that consumer jurisdiction does not apply in matters relating to torts; the only exception refers to an action in tort brought by a consumer that is indissociably linked to the contract actually concluded between that consumer and the seller or supplier.⁶⁷ However, this requires direct communication between the parties, where the professional makes misleading representations to induce the consumer to enter into a contract. In the case of standard communications to the market, as in the case of the publication of the key investment information sheet of the crowdfunding platforms, the provision of misleading, inaccurate, or incomplete information should not be considered indissociably connected with the conclusion of a contract.⁶⁸

With reference to the third condition, art 17 requires that the service provider pursues its activities in the Member State of the consumer’s domicile or, by any means, directs them to that Member State, and the contract falls within the scope of such activities (so-called ‘targeting activity test’). As clarified by the CJEU in *Pammer and Alpenhof*,⁶⁹ the mere accessibility of the trader’s (in this case, the service provider’s) or the intermediary’s website in the Member State in which the consumer is domiciled is not sufficient. Other pieces of evidence from which it may be concluded that the service provider’s activity is targeted to the Member State of the consumer’s domicile are required.⁷⁰ Elements which might be relevant for fintech digital platforms are, for instance, the use of the language and the payment currency of the Member State of the consumer’s domicile, as well as the direction of online marketing to the users of that country. For instance, an ICO might be considered as directing its activities towards a Member State on the basis of the language employed in the white paper, on

65 P Ortolani, (n 42).

66 Harald Kolassa (n 60) para 28. See P Ortolani (n 42) 332; I Kunda, ‘Crowdfunding in the EU: private international law issues by design’ in E Macchiavello (ed), *Regulation on European Crowdfunding Service Providers for Business* (Edward Elgar 2022) 537.

67 Case C–500/18, *AU C Reliantco Investments LTD e Reliantco Investments LTD Limassol Sucursala București* [2020] ECLI:EU:C:2020:264, para 73.

68 P Ortolani (n 42) 332–333.

69 Joined Cases C-144/09 and C-585/08, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v. Oliver Heller* [2010] ECR I-12527, para 69.

70 *ibid* para 93.

the currency used to buy tokens, and on the languages or extensions used by the website on which the white paper is published.⁷¹ To contrast, digital platforms may put in place technical measures with the aim to restrict the territories to which their activities are directed, for instance by disabling the registrations or transactions of users from certain countries on the basis of the IP address used.⁷² The targeting activity test is simpler with reference to crowdfunding platforms, as art 14 of Regulation (EU) 2020/1503 establishes a register of all crowdfunding service providers, with the indication of a list of the Member States in which the service provider has notified its intention to provide its activities. Henceforth, such a list precisely identifies the Member States where the crowdfunding service providers direct their activities for the purposes of art 17 Brussels I-bis Regulation. As a side effect, crowdfunding platforms might strategically exclude certain Member States from the list to avoid being sued before their jurisdiction (eg, by negatively assessing the length of proceedings).⁷³

3.3. Tortious jurisdiction

In matters relating to tort, delict or quasi-delict,⁷⁴ art 7(2) Brussels I-bis Regulation gives the investor the option to sue the service provider before the courts of the place where the harmful event occurred or may occur (*locus damni*). Whether the place of the happening of the event which may give rise to liability and the place where that same event results in damage are not identical, according to established CJEU case law, the harmful event is deemed to take place both in the place where the damage occurs and in the place where the events giving rise to that damage took place.⁷⁵ This hypothesis might occur when the information provided in the key investment information sheet pursuant to art 23 of Regulation (EU) 2020/1503 is allegedly misleading, incorrect, or incomplete, or in cases involving, for instance, alleged fraudulent misrepresentations inducing a transfer of crypto assets.⁷⁶

71 Some uncertainties might raise when, as often happens, the white paper has been written in English only, published on a common website extension (like .com), and the ICO presupposes an exchange among crypto tokens, not involving fiat currency. See I.M. Barsan, 'Legal Challenges of Initial Coin Offerings (ICO)' [2017] *Revue Trimestrelle de Droit Financier* 54, 64; B Steinrötter, 'International Jurisdiction and Applicable Law', in P Maume, L Maute, M Fromberg (eds), *The Law of Crypto Assets. A Handbook* (Beck Hart Nomos 2022) 71, 79.

72 I Kunda (n 66) 538.

73 *ibid* 329.

74 The concept of matters relating to tort, delict or quasi-delict within the meaning of art 7(2) Brussels I-bis covers all actions which seek to establish the liability of a defendant and are not matters relating to a contract. Among many, see Case C-167/00, *VKI v Karl Heinz Henkel* [2002] ECR I-08111, para 36.

75 Case 21/76, *Handelskwekerij G. J. Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR I-1735.

76 The pseudonymity of users on the DLT system does not hinder the identification of the *locus damni*. Even though the place where the events giving rise to the damage took place remains

On several occasions, the CJEU has been called to clarify what is the place where the damage occurs in case of financial loss. Nonetheless, the identification of the *locus damni* still leaves many questions unanswered.⁷⁷ First, the Court pointed out that this term cannot be interpreted “so extensively as to encompass any place where the adverse consequences can be felt of an event which has already caused damage actually arising elsewhere”.⁷⁸ In this vein, it does not refer to the place where the claimant is domiciled or where his assets are concentrated by reason only of the fact that he has suffered financial damage there resulting from the loss of part of his assets which arose and was incurred in another Member State (*Kronhofer*).⁷⁹ The mere fact that the applicant has suffered financial consequences does not justify the attribution of jurisdiction to the courts of the applicant’s domicile if both the events causing damage and the damage itself occurred in the territory of another Member State. Such an attribution of jurisdiction is justified if the claimant’s domicile is in fact the place in which the events giving rise to the damage took place or the damage occurred, namely the place where his bank account is established (*Kolassa*).⁸⁰ Nonetheless, in the absence of any other connecting factor, the place where the harmful event occurred ‘may not be construed as the place in a Member State where the damage occurred, when that damage consists exclusively of financial damage which materializes directly in the applicant’s bank account and is the direct result of an unlawful act committed in another Member State’ (*Universal Music*).⁸¹ Lastly, in a prospectus liability case, the Court identified some of the relevant circumstances that also contribute to attributing jurisdiction to the court of the place where is located the investor’s bank account. These are, for instance, the fact that the claimant, in connection with the financial transaction at issue, had dealings only with banks located in the same Member State, that the relevant prospectus had been notified to the supervisory bank of the same Member State, as well as that she signed in the same Member State the contract obliging her to make the investment, which has resulted in a definitive reduction in her assets (*Löber*).⁸²

unknown as the identity of the users, however the place where the damage occurs can be easily identified by the claimant.

77 Commission, Directorate-General for Justice and Consumers, Rass-Masson and others, *Study to support the preparation of a report on the application of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels Ia Regulation): Final Report*, (Publication Office of the European Union 2023), 274.

78 Case C-364/93, *Marinari* [1995] ECR I-2719, para 14.

79 Case C-168/02, *Rudolf Kronhofer v Marianne Maier and Otet al* [2004] ECR I-06009.

80 *Harald Kolassa* (n 60).

81 Case C-12/15, *Universal Music International Holding BV v Michael Tétreault Schilling, Irwin Schwartz, Josef Brož* [2016] ECLI:EU:C:2016:449.

82 Case C-304/17, *Helga Löber v Barclays Bank PLC* [2018] ECLI:EU:C:2018:701.

The circumstances identified by the CJEU case law on prospectus liability may be considered relevant also in crowdfunding-related disputes regarding allegedly misleading, incorrect, or incomplete information provided in the key investment information sheet. Unlike the prospectus, the key investment information sheet is not subject to verification or approval by competent authorities. Nonetheless, it must be made available ‘in at least one of the official languages of [the Member State where the investor is domiciled] or in a language accepted by the competent authorities of that Member State’ (art 23(3) of Regulation (EU) 2020/1503). This circumstance, together with the location of the investor’s bank account and the language used in the document, may be invoked to establish jurisdiction on the basis of art 7(2) Brussels I-bis.⁸³

4. Applicable law issues

Disputes arising from the cross-border provision of banking and financial services among European users generally fall under the scope of, respectively, Rome I Regulation on contractual obligations and Rome II Regulation on non-contractual obligations.⁸⁴ Both Regulations have similar limitations in material scope referring to financial instruments and the law of companies. Nonetheless, these exceptions, analysed below, have limited significance in relation to the identification of the law applicable to banking and financial platforms.

First, according to art 1(2)(d) Rome I Regulation and art 1(2)(c) Rome II Regulation, they do not apply to, respectively, contractual and non-contractual obligation ‘arising under bills of exchange, cheques and promissory notes and other negotiable instruments’, but only ‘to the extent that the obligations under such other negotiable instruments arise out of their negotiable character’. As a result, for negotiable instruments, such as stocks and bonds in the financial market, the exclusion only applies with regard to obligations arising out of their negotiable character. Furthermore, neither the contracts pursuant to which such instruments are issued nor contracts for the purchase and sale of such instruments are excluded.⁸⁵

Second, according to art 1(2)(f) Rome I and art 1(2)(d) Rome II Regulations, they do not apply to ‘questions governed by the law of companies and other bodies’. As a result, the law that is applicable to the rights and obligations arising from shares is not determined by the Regulations, since it is part of the

83 P Ortolani (n 42) 335.

84 Both Rome I and Rome II Regulations have universal application, meaning that the law they identify shall be applied whether or not it is the law of a Member State: see arts 2 Rome I and 3 Rome II.

85 M Giuliano, P Lagarde, ‘Report on the Convention on the law applicable to contractual obligations’ [1980] OJ C 282.

internal organization of the company. The conflict of laws rules of the law of the issuing company (*lex societatis*) apply. This might be the case with equity-based crowdfunding and ETOs (equity token offerings) platforms.

4.1. Contractual obligations

Rome I Regulation determines the law applicable to contractual obligations in situations involving a conflict of laws.⁸⁶ As the Regulation promotes party autonomy and freedom of choice, art 3(1) provides that ‘a contract shall be governed by the law chosen by the parties’. In the absence of a choice-of-law agreement,⁸⁷ art 4 lays down the criteria to determine the applicable law.

As most of the scenarios involving fintech platforms shall be generally qualified as provision of services, according to art 4(1)(b), the law of the country where the service provider has his habitual residence applies.⁸⁸ This is the case of the duties of information to the client that falls on the service provider. For instance, in relation to crowdfunding platforms, art 19 of Regulation 2020/1503 requires that crowdfunding platforms provide a series of information to investors, while art 20 of the same regulation imposes the annual disclosure of the default rates of the crowdfunding projects offered on their crowdfunding platform. Moreover, it might also refer to the duty to properly undertake the suitability assessment of investment services or financial instruments in investment advice or portfolio management services that fall on investment firms. According to art 54 of Regulation (EU) 2017/565, such responsibility shall not be reduced by the use of an electronic or AI system, as occurs in robo-advisor platforms.⁸⁹

86 As most of litigation scenarios involving fintech platforms does not refer to the content of the financial instrument, but on proprietary issues, namely who is the owner of the instrument, Rome I is generally applicable. See M Lehmann (n 13) 8.

87 On this point, see s 5 below.

88 As specified in recital n 17 of Rome I, ‘the concept of “provision of services” and “sale of goods” should be interpreted in the same way as when applying art 5 of Regulation (EC) No 44/2001 [Regulation Brussels I]’, now repealed by Brussels I-bis.

89 According to art 31 of Commission Delegated Regulation (EU) 2017/565 as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive [2016] OJ L 87, service provider’s civil liability is independent by the development of the algorithm in house or in outsourcing. This provision offers a strengthen protection to the investor, who, in case of outsourcing, shall not bring a tortious claim against the AI developer. Moreover, it overcomes the issues related to non-contractual civil liability claims for damage caused by AI-enabled products and services. On this point, see the proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) [2022] COM(2022) 496 final. However, for a peculiar example of non-contractual obligation involving a robo-advisor platform (called AFTAS) and a discussion of possible solutions, see British Institute of International and Comparative Law (BIICL), ‘Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations’ (2021) 79.

A different regime applies to contracts concluded within a ‘multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments’ (multilateral trading facility or MTF). To ensure uniformity in the terms and conditions of an issuance or an offer on such systems, art 4(1)(h) lays down the applicability of the same law that governs the MTF. This might be the case of robo advisors offering investment advice on financial instruments traded in an MTF system.

However, irrespective of the law applicable to the contract under the Regulation, art 9(1) imposes the application of ‘provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation’.⁹⁰ This provision might be of some relevance for fintech platforms, as financial markets are subject to rules that serve important public interests, such as preventing risks to the stability of the financial system. Examples of overriding mandatory provisions in finance are rules prohibiting money laundering, terrorism financing or tax evasion,⁹¹ as well as the financial market discipline regulated by the national rules implementing MiFID II.⁹²

4.1.1. *Consumer contracts*

For the purposes of the Rome I Regulation, financial services provided by a professional to a consumer (the investor) are subject to art 6, according to which the contract is governed by the law of the country where the consumer has his habitual residence.⁹³ The same conditions set out in art 17 Brussels I-bis Regulation for the consumer protection rule applies.⁹⁴

According to art 6(2), as Rome I Regulation promotes party autonomy and freedom of choice, the parties may freely choose another law applicable to the contract. However, such a choice may not deprive the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law of the country where the consumer has his habitual residence. This is the case of the information and exploration duties in relation to investment services under MiFID II.⁹⁵ In this connection, the national pro-

⁹⁰ See also *Unamar* (n 152).

⁹¹ M Lehmann, ‘Private international law and finance: nothing special?’ [2018] NIPR 3, 15.

⁹² M V Benedettelli, ‘Profilo internazionale della disciplina comunitaria dei mercati finanziari: la Direttiva MIFID tra conflitti di legge e conflitti di giurisdizione’ (2010) *Rivista di diritto societario*, 63.

⁹³ Recital n 26 of Rome I, which also specifies that ‘when a reference is made to terms and conditions governing the issuance or offer to the public of transferable securities or to the subscription and redemption of units in collective investment undertakings, that reference should include all aspects binding the issuer or the offeror to the consumer, but should not include those aspects involving the provision of financial services’.

⁹⁴ Recital n 24 of Rome I. See also s 3.2.

⁹⁵ M Lehmann (n 13) 15.

visions sanctioning a violation of the duties in art 24 MiFID II in relation to investment advice (including robo advisors) are mandatory provisions of the State of habitual residence of the investor-consumer. As a result, they may not be derogated by the choice of the parties.

Nonetheless, the consumer protection rule often does not apply to fintech platforms, due to the exceptions laid down in art 6(4). On the one hand, art 6(4) (e) excludes the application of consumer law to contracts concluded within an MTF system. On the other hand, art 6(4)(d) sets out that rights and obligations which constitute a financial instrument are not covered by the general rule applicable to consumer contracts. The aim is to avoid the application of different laws to each of the instruments issued, therefore changing their nature and preventing their fungible trading and offering.⁹⁶ In this vein, the special consumer regime is not applicable for investment and utility tokens with an investment focus.⁹⁷ However, the exclusion refers to the financial instrument itself and not to other contracts whose object is the financial instrument. In this vein, contracts for the purchase of financial instruments are not covered by this exclusion and are, therefore, subject to art 6.⁹⁸ Moreover, the same provision excludes the application of the consumer law to ‘rights and obligations constituting the terms and conditions governing the issuance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units in collective investment undertakings in so far as these activities do not constitute provision of a financial service’, to preserve the uniformity in the terms and conditions of an issuance or an offer. This might be the case with an ICOs (initial coin offerings) platform.

4.1.2. Applicable law in financial services related to crypto assets: a conundrum?

Major issues arise in determining the law applicable in financial services related to crypto assets, as transfers in DLT systems challenge the traditional concepts and methods of conflict of laws.⁹⁹ Crypto assets are intangible, have different financial features evolving in parallel with technological developments, have more than one usage spanning from payment to investment services, and have a cross-border reach, involving in the blockchain a multitude of anonymous actors.¹⁰⁰ In addition, conflict of laws norms operate principally on the

⁹⁶ Recital n 28 of Rome I.

⁹⁷ B Steinrötter (n 71) 71, 81.

⁹⁸ FJ Garcimartín Alférez, ‘The Rome I Regulation: Exceptions to the Rule on Consumer Contracts and Financial Instruments’ [2009] JPIL 85, 90.

⁹⁹ To date, ‘the analysis of the conflict of laws implications of crypto assets’ transactions is still in its infancy’: see B Steinrötter (n 71) 71, 72.

¹⁰⁰ A Dickinson, ‘Cryptocurrencies and the Conflict of Laws’, in D Fox and S Green (eds), *Cryptocurrencies* (n 58) 94, 97; C Bell and J Cainer, ‘Decrypting the Situs Conflicts of Laws Challenges in Cryptoasset Litigation’ (*Outer Temple Chamber*, 20 October 2020), 2-3 <<https://>

basis of territorial connecting factors, which presupposes the possibility of precisely locating acts and actors within the territory of a particular legal system.

The first point to consider relates to the question of the internationality of crypto assets transfers on the blockchain for private international law purposes. In particular, it is debated whether such transactions should be considered to be ‘intrinsically transnational’,¹⁰¹ or whether this should be verified on a case-by-case basis. In the latter case, a private international law analysis in all cases would be a costly and time-consuming exercise. In addition, the criteria traditionally used in private international law, such as the place of residence of the parties, have limited utility due to the anonymity of the actors operating on the blockchain. Furthermore, the identification of pre-set and precisely criteria of internationality does not suit the blockchain universe, which is characterised by its flexible and fast-evolving nature.¹⁰²

Moreover, there is no uniformity in the classification of crypto assets. First, it is debated whether crypto assets that are used in contractual relations as remuneration could be classified as currency for the purposes of private international law. Consequently, the *lex monetae* (law of the Country issuing the currency) would apply, thus raising some difficulties, as crypto assets are normally not issued by States.¹⁰³ Second, digital assets have been considered as a ‘distinct third category of personal property’,¹⁰⁴ leading to the application of the connecting factor used in the area of international property law, namely the *lex situs* (law of the country where the property is located).¹⁰⁵ However, this solution collides with the difficulties in localisation of the crypto asset in DLT systems, deriving

www.outertemple.com/wp-content/uploads/2020/10/Decrypting-the-Situs.pdf> accessed 30 May 2024.

101 On the international nature of the blockchain, see F Guillaume, ‘Aspects of private international law related to blockchain transactions’, in D Kraus, T Obrist, O Hari (eds), *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law* (Edward Elgar 2019) 59.

102 B Yüksel Ripley, ‘When is a cryptocurrency transfer international in distributed ledger technology-based systems?’ (2023) EU and Comparative Law Issues and Challenges Series (ECLIC) 196.

103 F Krysa, ‘Taxonomy and Characterisation of Crypto Assets’, in A Bonomi, M Lehmann, S Lalani (eds), *Blockchain and Private International Law* (Brill 2023) 203. Nonetheless, El Salvador and the Central African Republic recently adopted the bitcoin as a legal tender. See B Yüksel Ripley, ‘The Law Applicable to Crypto Assets: What Policy Choices Are Ahead of Us?’, in A Bonomi, M Lehmann, S Lalani (eds), *Blockchain and Private International Law* (Brill 2023) 266 ff.

104 Law Commission, *Digital assets: Consultation paper* (Law Com, No 256, 28 June 2022) 69.

105 This is the approach adopted by English scholars; among many, see Financial Markets Law Committee (FMLC), ‘Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty’ (2018) <http://fmllc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 3 July 2023, paras 4.4–4.8; UK Jurisdiction Taskforce, ‘Legal statement on crypto-assets and smart contracts’ (*Tech Nation*, November 2019), 49–57; A Dickinson, ‘Cryptocurrencies and the Conflict of Laws’, in D Fox and S Green (eds), *Cryptocurrencies* (n 58) 94, 126.

from their decentralised and distributed nature.¹⁰⁶ Similar issues emerge also in relation to other types of intangibles with no physical location, such as money debts, shares, rights of action, and intellectual property. In these cases, conflict of laws solutions have been developed ascribing them to an artificial or fictional legal situs where they can be pursued or enforced. Nonetheless, such a solution has not been developed yet for crypto assets.¹⁰⁷ Finally, it has been argued that crypto assets could be assimilated into a form of intangible property, which consists of a 'bundle of 'entitlements' arising by reason of participation' in the blockchain.¹⁰⁸ In this vein, entitlements established between the participants of the blockchain (assignors) and investors (transferees) for the assignment of crypto assets might fall under the conflict of laws rules on assignments. Unfortunately, the scope of application of the blockchain is much wider than that of assignment, as the transfer of intellectual property rights or transfer physical assets, whether movables or immovables, through tokenization.¹⁰⁹

As a result, the existing private international law legal framework does not fit for the purpose of ensuring legal certainty in the determination of applicable law related to crypto assets.¹¹⁰

Such a conundrum also afflicts the EU private international law legal framework. Whilst the possibility to encompass a unitary approach through the

106 Financial Markets Law Committee (FMLC), 'Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty' (2018) <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 3 July 2023, paras 6.1–6.28.

107 B Yüksel Ripley, 'The Law Applicable to (Digital) Transfer of Digital Assets: The Transfer of Cryptocurrencies via Blockchains?' in MM Fogt (ed), *Private International Law in an Era of Change* (Edward Elgar 2024); F Villata, L Válková, 'Property Rights Over Cryptocurrencies: A Conflict-Of-Laws Perspective' (2023) EU And Comparative Law Issues and Challenges Series 53ff.

108 This is the approach taken in the Swiss Federal Act to Adapt Federal Law to Developments in Distributed Ledger Technology ('DLT' Act'), see *Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 25. September 2020*, RO 2021 33.

109 M Lehmann, 'Who Owns Bitcoin? Private Law Facing the Blockchain' (2019) EBI Working Paper Series No 42, 17 <Lehmann, Matthias, Who Owns Bitcoin? Private Law Facing the Blockchain (June 11, 2019). 21 Minn. J.L. Sci. & Tech. 93 (2019), European Banking Institute Working Paper Series 2019 – no. 42, <<https://ssrn.com/abstract=3402678>> accessed 30 May 2024; C Bell and J Cainer (n 100), 13.

110 In January 2023, the International Institute for the Unification of Private Law (UNIDROIT) launched a public consultation regarding a set of 'Draft Principles and Commentary on Digital Assets and Private Law', UNIDROIT 2023 Study LXXXII – PC; for a preliminary overview, see M Lehmann, 'Private International Law in the Proposal by the UNIDROIT Working Group on Digital Assets' (*EAPIL blog*, 1 February 2023) <https://eapil.org/2023/02/01/private-international-law-in-the-proposal-by-the-unidroit-working-group-on-digital-assets/> accessed 30 May 2024. Moreover, in March 2023, a joint project among the Hague Conference of Private International Law and UNIDROIT on this topic has been launched; see HCCH Council of General Affairs and Policy, 'HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens' (March 2023) prel doc No 3C.

adoption of a single law to the DLT system would have solved the problem at its roots,¹¹¹ however, this option cannot arise from the application of the rules of the Rome I Regulation. The single law applicable to MTF systems according to art 4(1)(h) cannot generally operate in relation to the blockchain.¹¹² Eventually, it applies to the operation of a trading platform for crypto-assets, as it is deemed equivalent to the operation of a multilateral trading facility.¹¹³ Therefore, under the Rome I Regulation, different conflict of laws norms apply on the basis of the type of transaction under analysis.

Financial transactions which involve the transfer of tangible goods in exchange for units of a cryptocurrency might be classified as a contract for the sale of goods under 4(1)(a) Rome I.¹¹⁴ As a result, the law of the country where the seller has his habitual residence applies. In this vein, the use of cryptocurrency as the medium of exchange does not present particular difficulties in terms of the identification of applicable law.¹¹⁵

Greater concerns emerge in the remaining hypotheses. The criteria of the law of the habitual residence of the service providers, laid down by art 4(1)(b), leaves uncertainty, due to the multiple service providers, spread in different countries, participating in the blockchain. The same issues arise in relation to art 4(2), according to which, where the contract is not covered by art 4(1), the 'law of the country where the party required to effect the characteristic performance of the contract has his habitual residence' applies, and art 4(4), according to which 'the law of the country with which it is most closely connected' applies.¹¹⁶

111 To contrast, for the applicability of a unitary approach ('one-system-one-law') to permissioned cryptocurrency systems, see B Yüksel Ripley, 'Cryptocurrency Transfers in Distributed Ledger Technology-Based Systems and Their Characterisation in Conflict of Laws', in J Borg-Barthet and others (eds), *From Theory to Practice in Private International Law* (Bloomsbury Publishing 2024); the Author investigates on the applicability of a unitary approach ('one-system-one-law') to permissioned cryptocurrency systems, and of a segmented approach for permissionless in an analogy to EFTs (electronic funds transfers). For a scholarly suggestion for applying the *lex fori* as an option in the absence of a better solution, see F Guillaume, 'Aspects of private international law related to blockchain transactions', in D Kraus, T Obrist, O Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar 2019) 49, 79.

112 A Dickinson, 'Cryptocurrencies and the Conflict of Laws', in D Fox and S Green (eds), *Cryptocurrencies* (n 58) 94, 111.

113 Art 60(3)(b) MiCA Regulation.

114 The same considerations apply with regards to art 7(1)(a) Brussels I-bis, in relation to the identification of forum law.

115 A Dickinson, 'Cryptocurrencies and the Conflict of Laws', in D Fox and S Green (eds), *Cryptocurrencies* (n 58) 93, 98; G Rühl, 'Smart (legal) contracts, or: Which (contract) law for smart contracts?', in B Cappiello and G Carullo (eds), *Blockchain, Law and Governance* (Springer 2020) 170.

116 A Dickinson, 'Cryptocurrencies and the Conflict of Laws', in D Fox and S Green (eds), *Cryptocurrencies* (n 58) 93, 112. Regarding the opportunity to apply the escape clause of art 4(3) Regulation Rome I, see B Steinrötter (n 71) 71, 83.

4.2. Non-contractual obligations

Rome II Regulation applies to cross-border disputes arising from non-contractual obligations, as in the case of alleged violations of prospectus rules.¹¹⁷ For instance, in crowdfunding platforms, this hypothesis might occur when the information provided in the key investment information sheet pursuant to art 23 of Regulation (EU) 2020/1503 is allegedly misleading, incorrect, or incomplete. The Regulation has also been applied in a situation involving the fraudulent transfer of millions of dollars worth of cryptocurrency performed by hackers against a cryptocurrency exchange.¹¹⁸

In the absence of a choice-of-law agreement,¹¹⁹ the general rule laying down the criteria to determine the law applicable to a non-contractual obligation arising out of a tort applies. However, Regulation Rome II does not provide special conflict of laws rules for financial torts, leaving many questions on the law applicable to this matter still unsolved.¹²⁰

According to art 4(1), this is the law of the country in which the damage (namely, the financial loss) occurs, ‘irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur’. This provision shall be interpreted consistently with art 7(2) Brussels I-bis, referring to tortious jurisdiction,¹²¹ and the related CJEU case law.¹²² As mentioned before,¹²³ the Court identified the country where the financial loss occurred on the basis of ‘a combined multifactor test with variable criteria’,¹²⁴ depending on circumstances linked to each individual investor. Such an approach favours flexibility to the detriment of legal certainty, as makes potential liability unforeseeable for the tortfeasor.¹²⁵

117 Arguing that investment tokens can be classified as securities and, as a consequence, EU initial disclosure regulation applies to ICOs, requiring the issuer to draw up a prospectus, see P Maume, ‘Initial Coin Offerings and EU Prospectus Disclosure’ [2020] 185, 191.

118 *LMN v. Bitfyer Holdings Inc and others* [2022] EWHC 2954 (Comm), 29 November 2022.

119 On this point, see s 5 below.

120 On the opportunity of reforming Rome II so as to add a special conflict rule for financial torts, see M Lehmann (n 13) 25; F Rielaender, ‘Financial torts and EU private international law: will the search for the place of “financial damage” ever come to an end?’ [2022] JPIL 28, 53; British Institute of International and Comparative Law (BIICL), ‘Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations’ (2021) 33.

121 Recital n 7 of Rome II.

122 *Universal Music* (n 81); Case C-304/17, *Helga Löber v Barclays Bank PLC* (n 82).

123 See para 3.3.

124 M Lehmann (n 13) 18.

125 Art 4(1) has been also applied in a situation involving the fraudulent transfer of millions of dollars-worth of cryptocurrency performed by hackers against a cryptocurrency exchange. The High Court of Justice of England and Wales identified the *locus damni* in England, as this was the place where the relevant cryptocurrencies were located at the time of the hack, as this is the place of incorporation of the exchange damaged and where it conducts its main

The application of art 4(2) causes another issue. It sets out that, if both parties have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply. This provision might give rise to a distortion that contrasts with the principle of equal investor treatment.¹²⁶ Therefore, the application of this norm is not appropriate for a harmonized internal capital market.¹²⁷

art 4(3) states that, if the tort is manifestly more closely connected with a country other than that determined through arts 4(1) or 4(2), the law of that other country shall apply. On first scrutiny, this provision seems to overcome fragmentation issues and legal uncertainty by applying the same law to all financial torts committed by the same issuer or on the same market. However, it is not the proper device for achieving such a goal. On the one hand, as an exception clause, this norm should not be used to regulate an entire category of torts, such as financial torts.¹²⁸ On the other hand, the criterion of close connection gives rise to different interpretations, spanning from the law of the country where the issuer has its registered office to the law of the place where the relevant market is located, or, where relevant, the home country as defined under the rules for prospectus approval.¹²⁹

It is disputed in legal doctrine whether prospectus liability might be qualified as *culpa in contrahendo*, regulated by art 12 Rome II. On the one hand, recital n 30 Rome II seems to support this position as qualifies ‘the violation of the duty of disclosure’ as pre-contractual liability. The advantage of such a characterization is that the conflict rules for contractual relationships would be applicable. On the other hand, the text of art 12 Rome II does not fit with prospectus liability cases, as refers to obligations arising out of ‘dealings prior to the conclusion of a contract’. Generally, the issuer and the investor have no contact before the acquisition of the security.¹³⁰

5. Agreements on jurisdiction and applicable law

In the vast majority of cases, the general terms and conditions of banking and financial platforms include choice-of-court and choice-of-law clauses. Such

business. In addition, this is also where the financial loss took place, as the cryptocurrencies was taken from the exchange’s control See *LMN v. Bitfyer Holdings InC and others* [2022] EWHC 2954 (Comm), 29 November 2022, par. 20.

126 M Lehmann (n 13) 18.

127 B Steinrötter (n 71) 71, 101.

128 M Lehmann (n 13) 23.

129 Among many, see M Lehmann, ‘Prospectus Liability and Private International Law Assessing the Landscape after the CJEU’s Kolassa Ruling (Case C–375/13)’ [2016] JPIL 318, 325–326; M Gargantini, ‘Prospectus Liability’ (n 61) 453–454.

130 M Lehmann, ‘Prospectus Liability’ (n 129) 338; M Gargantini, ‘Prospectus Liability’ (n 61) 454.

clauses provide legal certainty and foreseeability on the service provided, with mutual benefits for the parties. Moreover, as national legal systems adopt significantly different regimes on banking and financial matters, these agreements might ensure that potential disputes are decided by the court and on the basis of the law which is better equipped to deal with that particular type of legal relations.

5.1. Choice-of-court agreements

The parties, irrespective of their domicile, can determine the jurisdiction of ‘a court or the courts of a Member State’ by concluding a choice-of-court agreement. In this case, according to art 25 Brussels I-bis, the jurisdiction shall be exclusive unless the parties have agreed otherwise. An additional advantage of choice-of-court agreements is the derogation from the *lis pendens* mechanism so that the chosen court, according to art 31(2), will not have to stay the proceedings, even when it is not the court first seized.¹³¹

To meet the formal requirements listed in art 25(1) Brussels I-bis, the contract signed by the parties shall contain an express reference to those general conditions and shall be checked by a party exercising reasonable care.¹³² This is possible also using ‘a communication by electronic means which provides a durable record of the agreement’. This is the case of jurisdiction clauses included in the general terms and conditions of a contract concluded by ‘click-wrap-ping’, as often happens in digital platforms. As clarified by the CJEU, this method fulfils the in-writing requirement of art 25(1)(a) Brussels I-bis when it makes it possible to print and save the text of those terms and conditions before the conclusion of the contract.¹³³ Crowdfunding platforms deserve a different analysis, as jurisdiction agreements are generally included in the key investment information sheet that the crowdfunding service provider is obliged to publish, according to art 23 of Regulation 2020/1503. Whether considering the key investment information sheet analogous to the prospectus, the CJEU case law on jurisdiction clauses contained in the prospectus applies. In *Profit Investment*,¹³⁴ the CJEU stated that where the choice-of-court clause is included in the prospectus concerning the issue of bonds, the in-writing requirement is met only if the contract signed by the parties on the primary market expressly mentions the acceptance of that clause or contains an express reference to that prospectus. In crowdfunding, this would require that the contract concluded between the

131 P Ortolani (n 42) 337.

132 Case 24/76, *Estasis Salotti di Colzani Aimo et Gianmario Colzani v Riiva Polstereimaschinen GmbH* [1976] ECR I-1832.

133 Case C-322/14, *El Majdoub v CarsOnTheWeb* [2015] ECLI:EU:C:2015:334, para 40; for similar conclusions on art 23(1)(b) and (c) of the 2007 Lugano Convention, see Case C-358/21, *Tilman SA c Unilever Supply Chain Company AG* [2022] ECLI:EU:C:2022:923, para 59.

134 Case C-366/13, *Profit Investement v Ossi et al* [2016] ECLI:EU:C:2016:282.

investor and the project owner should contain an express reference to the jurisdiction clause in the key information sheet.¹³⁵ In the absence of this condition, it is not excluded that the insertion of a jurisdiction clause into a prospectus (ie the key investment information sheet in crowdfunding platforms) concerning the issue of bonds may be regarded as a form which accords with a usage in international trade or commerce, for the purpose of art 25(1)(c) Brussels I-bis.¹³⁶ Hence, two conditions are required. First, such conduct must be generally and regularly followed by project owners in the same sector. Second, the parties must have previously had financial relations between themselves or with other parties, or the conduct in question must be sufficiently well known to be considered an established practice. The latter hypothesis might apply to crowdfunding platforms as well.

Jurisdiction agreements choosing the court of a third State are outside the scope of Brussels I-bis Regulation. Whether a European user is involved, and the choice falls on a court of Iceland, Norway or Switzerland, the rules of the 2007 Lugano Convention apply. In the same vein, the jurisdiction agreement is governed by the provisions of the Hague Convention of 2005 when it identifies the courts of Mexico, Montenegro, Singapore or the United Kingdom. However, this convention does not apply to consumer contracts.¹³⁷ In the remaining hypotheses, the private international law norms of the court in which the action is brought (*lex fori*) apply.

5.1.1. Restrictions to jurisdiction agreements

Party autonomy is not without limitation, as art 25(4) Brussels I-bis lays down restrictions to the legal force of jurisdiction agreements in specific cases. In particular, the provisions referring to exclusive jurisdiction and consumer contracts might be relevant for fintech digital platforms.

On the one hand, choice-of-court clauses have no legal force if the courts whose jurisdiction they purport to exclude have exclusive jurisdiction by virtue of art 24. Such a hypothesis may occur in equity-based crowdfunding and ETOs (equity token offerings) platforms, which both concern the offering of venture capital.

On the other hand, a special procedural regime applies to consumer contracts. Art 19 Brussels I-bis limits party autonomy to avoid the choice-of-court clause derogating the rules of jurisdiction more favourable to the interests of consumers, who are considered weaker parties in the dispute. Jurisdiction agreements are admitted in three hypotheses, which drastically restrict the scope of application of such norms to Fintech digital platforms. First, according to art

¹³⁵ I Kunda (n 66) 535–536.

¹³⁶ *Profit Investment* (n 134) para 50.

¹³⁷ Art 2(1)(a) of the 2005 Hague Convention.

19(1)(a), the jurisdiction agreement shall be entered into after the dispute has arisen. As this means the consumer gives up the more favourable jurisdiction of the court of the Member State where he is domiciled, this case has limited practical application. Second, according to art 19(1)(b), the agreement allows the consumer to bring proceedings in courts other than those indicated in the Regulation. However, this would be in clear contrast with the interest of the professional (the service provider), who might aim at concentrating all litigations in a single forum.¹³⁸ Third, according to art 19(1)(c), the agreement chooses the law of the Member State where both the parties are, at the time of conclusion of the contract, domiciled or habitually resident.

The restrictions related to jurisdiction agreements in consumer contracts might also derive from consumer protection law, namely Directive 93/13/EEC (Unfair Contract Terms Directive or UCTD).¹³⁹ Art 3(1) UCTD establishes that ‘a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer’. This also includes clauses restricting the consumer’s right to take legal action, such as a choice-of-court agreement which establishes the exclusive jurisdiction of the service provider’s domicile. Hence, such an agreement obliges the consumer to submit to the exclusive jurisdiction of a court which may be a long way from his domicile, making it difficult for him to enter an appearance.¹⁴⁰ The national court in which the action is brought is required to examine, of its own motion, the unfairness of a contractual term with an assessment on a case-by-case basis.¹⁴¹ Consequently, it has been contended that, if the unfairness of the jurisdiction clause is established, the choice-of-court clause is invalid while the default rule of art 18(1) Brussels I-bis applies.¹⁴² Such a position seems to be in line with the Court of Justice ruling *DelayFix*, according to which the substantial validity of a jurisdiction clause is to be assessed in the light of the national law of the court designated in the jurisdiction clause interpreted in accordance with the Unfair Contract Terms Directive.¹⁴³

¹³⁸ P Ortolani (n 42) 322.

¹³⁹ Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95.

¹⁴⁰ Joined Cases C–240/98 and C–244/98, *Océano Grupo Editorial SA* [2000] ECR I-4963, para 22.

¹⁴¹ Case C-243/08, *Pannon GSM Zrt. v Erzsébet Sustikné Győrfi* [2009] ECLI:EU:C:2009:350, para 35.

¹⁴² A Bonomi ‘Jurisdiction over consumer contracts’ in A Dickinson and E Lein (eds), *The Brussels I Regulation Recast* (OUP 2015) 236. A similar position seems to be at the basis of the analysis presented in I Kunda (n 66) 539. A different position affirms that the UCTD takes priority over the Brussels I-bis Regulation according to art 67 Brussels I-bis: see P Mankowski ‘Article 19’ in P Mankowski and U Magnus (eds), *Brussels Ibis Regulation: Commentary* (Otto Schmidt 2023) 522.

¹⁴³ Case C–519/19 *Ryanair DAC* ECLI:EU:C:2020:933, para 49 ff.

However, such a position has been criticized, as it has been argued that the *DelayFix* case does not define the relationship between the regime of consumer jurisdiction in the Brussels I-bis Regulation and consumer protection resulting from the Unfair Contract Terms Directive. Hence, the circumstances of the case, which refers to a contract of carriage, are outside the scope of application of the art 17 Brussels I-bis. In this vein, the Court did not intend to justify that the jurisdiction clause in a consumer contract will always be subject to double limitations, both under procedural law (Brussels I-bis Regulation) and substantive law (Unfair Contract Terms Directive). On the contrary, it was the impossibility to apply the guarantees provided by the Brussels I-bis Regulation for consumer contracts in that specific case, ie a contract of carriage, that justified examination of the substantive validity of the jurisdiction clause contained in a consumer contract in the light of the Unfair Contract Terms Directive, as a sort of last safeguard.¹⁴⁴

5.2. Choice-of-law agreements

According to art 3 and art 14 Rome II Regulation, choice-of-law agreements might refer also to the law of a third State, due to the universal application of both Regulations. Hence, any law chosen shall be applied whether or not it is the law of a Member State. The agreement can be expressed or tacit. According to art 3(1) Rome I Regulation, a tacit agreement exists for contractual matters if clearly demonstrated by the terms of the contract or the circumstances of the case, and, according to art 14(1) for non-contractual matters if demonstrated with reasonable certainty by the circumstances of the case. While the chosen law usually applies in contractual matters, however, this rarely happens in non-contractual matters, as the event giving rise to the damage is usually unpredictable and fortuitous.

Rome I Regulation expressly promotes party autonomy and freedom of choice, whether art 3(1) provides that ‘a contract shall be governed by the law chosen by the parties’. That choice can either refers to ‘the whole or to part only of the contract’.

Rome II Regulation allows the parties to submit non-contractual obligations to a chosen law in two different hypotheses, which drastically restrict the scope of application of this norm to fintech digital platforms. On the one hand, according to art 14(1)(a), the agreement shall be concluded after the event giving rise to the damage occurred. Although it is not excluded that a subsequent agreement might intervene between the parties, such a hypothesis is destined to have limited practical application. On the other hand, according to art 14(1)(b), the agreement shall be concluded also before the event giving rise to the

¹⁴⁴ B Wołodkiewicz ‘The Enforceability of a Jurisdiction Clause against an Assignee’ (2021) *Journal of European Consumer and Market Law* 210.

damage occurred, but at the double condition that all the parties are pursuing a commercial activity and the agreement has been freely negotiated. Such conditions rarely apply to fintech platforms. First, this hypothesis does not apply to consumer contracts, as both actors must pursue a commercial activity. Second, digital platforms generally include choice-of-law clauses in general terms and conditions' standard documents. This does not automatically exclude that the clause has been freely negotiated by the parties; however, it must have been the specific object of negotiations among the parties.¹⁴⁵ A similar hypothesis is very unlikely in fintech platforms, where disintermediation prevails.¹⁴⁶

5.2.1. *Restrictions to applicable law agreements*

Limitations to party autonomy touch upon both contractual and non-contractual matters. General restrictions refer to the applicability of the mandatory provisions of the law of the country with which it is most closely connected with the obligation, or the traditional private international law limitations to protect the public interest, namely overriding mandatory rules and public policy.

On the one hand, the choice of the parties does not prejudice the application of the mandatory provisions of the law of the country with which the situation is most closely connected with the obligation.¹⁴⁷ As a result, a choice-of-law clause cannot deprive the investor of the protections afforded by the mandatory provisions of the State of his habitual residence. The same principle applies when all the elements relevant to the situation are located in the EU, but the parties have chosen the law of a third country. In such cases, the choice of the parties does not prejudice the application of the mandatory provisions of EU law.¹⁴⁸ In crowdfunding platforms, this might be the case of the right of the non-sophisticated investor to revoke his offer to invest during a pre-contractual reflection period established by art 22 of Regulation 2020/1503, which purports to strengthen the protection for non-sophisticated investors.¹⁴⁹

On the other hand, overriding mandatory norms and public policy of the forum justifies the disapplication of the law identified by the provisions of Rome I and Rome II Regulations, including the law chosen by the parties. More precisely, overriding mandatory provisions are norms of the law of the forum which are applicable to any situation falling within their scope, irrespective of

145 M Magnus and P Mankowsky (eds), *Rome II Regulation: Commentary* (Verlag Dr. Otto Schmidt 2019), 502.

146 In particular, with reference to ICOs, see FJ Garcimartín Alférez and S Sánchez Fernández, 'Is private international law tech-proof? Conflict of laws and FinTech: selected issues', in T John, R Gulati, and B Koehler (eds), *The Elgar Companion to the Hague Conference on Private International Law* (Edward Elgar 2020) 406, 415.

147 Arts 3(3) Rome I and 14(2) Rome II.

148 Arts 3(4) Rome I and 14(3) Rome II.

149 I Kunda (n 66) 544.

the law otherwise applicable to the contract.¹⁵⁰ Their conceptualisation should be construed more restrictively than that of mandatory provisions, as their respect is ‘regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation’.¹⁵¹ It is for the national court hearing the case ‘to take account not only of the exact terms of that law, but also of its general structure and of all the circumstances in which that law was adopted in order to determine whether it is mandatory in nature in so far as it appears that the legislature adopted it in order to protect an interest judged to be essential by the Member State concerned’.¹⁵² Examples of overriding mandatory provisions in the area of finance are rules prohibiting money laundering, terrorism financing or tax evasion.¹⁵³ The overriding mandatory provisions of the forum State are applicable in both contractual and non-contractual matters, according to arts 9(2) Rome I Regulation and 16 Rome II Regulation. To contrast, such rules of the law of the country of the place of performance are applicable only in contractual matters, according to art 9(3) Rome I. Moreover, the public policy mechanism allows the national court to refuse the application of a provision of the law of any country specified by the Regulations. Arts 21 Rome I Regulation and 26 Rome II Regulation condition this refusal to the manifest incompatibility with the public policy of the forum, meaning that the provision infringes a fundamental principle of the law of the forum.

Finally, special restrictions apply to consumer contracts. As analysed above, art 6(2) Rome I Regulation establishes that the choice of the parties may not deprive the consumer of the protection afforded to him by the mandatory provisions of the law of the country where the consumer has his habitual residence. In addition, in *VKI v. Amazon*,¹⁵⁴ the CJEU clarified that a choice-of-law clause inserted in the general terms and conditions, which has not been individually

150 Member States’ national courts have adopted different approaches on the distinction between overriding rules and non-derogable rules. Among many, see M Wilderspin, ‘Overriding Mandatory Provisions’, in J Basedow and others (eds), *Encyclopedia of Private International Law* (Edward Elgar 2017) 1331–1332.

151 Art 9(1) Rome I. According to the Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I) COM (2005) 650 final, 7, this definition is based on a judgment of the CJEU, namely Joined Cases C–369/96 and C–376/96, *Arblade* [1999] ECR I-8498, para 30.

152 Case C–184/12, *United Antwerp Maritime Agencies (Unamar) NV v Navigation Maritime Bulgare* [2013] ECLI:EU:C:2013:663, para 50, with reference to art 9 Rome I; Case C–149/18, *Agostinho da Silva Martins v Dekra Claims Services Portugal SA* [2019] ECLI:EU:C:2019:84, para 31, with reference to art 16 Rome II.

153 M Lehmann (n 13) 15. On the opinion that an overriding mandatory provision which aims to protect the stability of a financial system is different from other overriding mandatory provisions, see AJ Berends, ‘Why overriding mandatory provisions that protect financial stability deserve special treatment’ [2014] NILR 69.

154 Case C–191/15, *Verein für Konsumenteninformation (VKI) v Amazon EU Sàrl* [2016] ECLI:EU:C:2016:612, para 71.

negotiated by the parties, shall inform the consumer that under art 6(2) he also enjoys the protection of the mandatory provisions of the law of his habitual residence. Otherwise, it is considered unfair under the Unfair Contract Terms Directive in so far as it leads the consumer into error by giving him the impression that only the law of that Member State applies to the contract. *De facto*, the CJEU, in a criticised expression of so-called judicial activism,¹⁵⁵ introduced a duty to inform the consumer about the more favourable law principle enshrined in art 6(2), which has limited practical relevance. Hence, the consumer would rarely rely on the unfairness (and consequent invalidity) of the choice-of-law clause, which deprives the consumer of any possibility of relying on a chosen law that is more favourable to him than the law of his habitual residence.¹⁵⁶

6. Conclusion

Analysing the cross-border provision of banking and financial services through digital platforms means dealing with the peculiarities of the application of conflict of laws rules in two different areas of law, respectively, the digital arena and finance. As a result, the application of the existing EU private international law legal framework presents multiple layers of difficulties.

First, it is necessary to contemporarily consider the specificities of the EU conflict of laws rules in both the digital realm and the financial market. A paradigmatic example is the application of the consumer regime to fintech platforms' users, in particular, the issue of qualification of the investor as a consumer. On the one hand, the EU private international law legal framework has not been adapted to the digital environment but has remained technologically neutral. As a result, the task to adjust the traditional EU conflict of laws rules to the specific problems of online platforms fell upon the CJEU.¹⁵⁷ On the other hand, in relation to financial contracts, the fungibility of financial instruments as a necessary condition for trading and the principle of investor equality requires the application of a single law to all the transactions entered into on an exchange. The same principles also exclude the operability of the consumer regime to financial instruments, as this would lead to a fragmentation of

155 G Rühl, 'The unfairness of choice-of-law clauses, or: The (unclear) relationship Between Article 6 Rome I Regulation and the Unfair Terms in Consumer Contracts Directive: VKI v. Amazon' (2018) CMLRev 220.

156 P Mankowski, 'Just how free is a free choice of law in contract in the EU? (2017) JPIL 248; G-P Calliess and M Renner (eds), *Rome Regulations: Commentary* (Wolters Kluwer 2020) 98.

157 J Hörnle and I Revolidis, 'Civil and Commercial Cases in the EU: Jurisdiction, Recognition, and Enforcement, Applicable law – Brussels Regulation, Rome I and Rome II Regulations', in J Hörnle, *Internet Jurisdiction Law and Practice* (OUP 2021) 264; P Franzina, 'Promoting Fairness and Transparency for Business Users of Online Platforms', in I Pretelli (ed), *Conflict of Laws in the Maze of Digital Platforms / Le droit international privé dans le labyrinthe des plateformes digitales* (Schulthess 2018) 147.

applicable law depending on the investor's habitual residence. Hence, the latest developments of the relevant CJEU case law on consumers in the digital market and the special rules of Brussels I-bis Regulation related to the financial market likewise apply to fintech platforms.

Second, in both areas, some critical issues are still unsolved, leaving space for legal uncertainty for European users. Therefore, even though the CJEU case law offers some guidance, some grey zones remain. This is the case, for instance, of the identification of applicable law to financial services related to crypto assets.

Third, the intersection of these two areas, ie the digitalisation of the financial market, adds new complexity to pre-existing conflict of laws issues. This applies to the localisation of purely financial loss in torts, where the dematerialisation of the place of damage poses new challenges in the application of (*per se* still problematic) traditional private international law rules. Hence, the Rome II Regulation's regime, which favours the application of the law of the place of the damage and of the common domicile of the tortfeasor and victim, is now considered ill-fitted for the securities context. Therefore, the absence of a special conflicts rule for financial torts, able to tie private liability to the market affected, raises major concerns.

In conclusion, the current EU private international law legal framework is gradually adapting to the new challenges of technological progress in digital finance, in the attempt to guarantee the reasonable foreseeability of forum and applicable law issues emerging from the widespread diffusion of fintech platforms among European users. Major issues refer to still existing legislative gaps referring to the absence of special conflicts rule for financial torts, as well as to legal uncertainties referring to crypto assets. Nonetheless, greater caution is needed with reference to the adoption of specific legislative reforms dedicated to private international law norms in digital finance. As technology progresses much faster than law, in this sector legal interventions risk becoming obsolete before their own entry into force, thus undermining legal certainty instead of ensuring it.

A New Form of Working Relationship in The Digital Age: Crowdfunding from a Private International Law Perspective

*Esra Tekin **

Dicle University Faculty of Law, Turkey
ORCID 0000-0003-0081-9000

DOI: 10.54103/milanoup.215.c452

Abstract

Among the most important working life innovations brought about by the technological developments are the new working relations. They differ significantly in their structure, compared to the classical contract types. Crowdfund, a sub-title of platform work, is among them. It is a way of working through the platform where customers and service providers meet over the internet. There is a trilateral relationship in crowdfunding: the user (principal), the web-platform and the user (worker). In some crowdfund relationships, the work activity is performed completely on the computer and on the Internet, while in others the work activity is performed in the physical world. Crowdfund raises conflicting issues in terms of private international law. With crowdfund the company or person who is ordering work could be located in one state, the platform itself could be located in another state, and the workers could be located in many other states. In addition, crowdfund companies are often multinational companies. This new business relationship with an international element clearly falls within the scope of private international law. Crowdfunding is characterized differently in different jurisdictions. Currently, cases are being heard around the world on the question of whether crowdfunders are “employees” or “independent contractors”. It is mainly the aspects of substantive law that interest legal doctrine. However, questions of private international law are central. My study seeks to answer the question of whether current conflict of laws rules can respond to technological developments. Large multinational companies (e.g. Uber, Deliveroo.) are fighting against a recharacterization of their activities as employment relationships, on the grounds that their business model would not be profitable in this case. “Workers” are bound by standard

* Dicle University Faculty of Law, Diyarbakır, Türkiye, tekinesra@outlook.com.tr, Orcid: 0000-0003-0081-9000.

contracts containing choice of court and choice of law clauses which they can not negotiate and which de facto prevent them from bringing legal proceedings. These issues are worth examining in depth from a comparative law perspective. In addition, other types of “employment relationships” are formed solely on the internet, through internet platforms, which makes it difficult to attach these activities to a particular state. For this type of fundamentally international legal relationship, it is necessary to rethink the criteria of international jurisdiction of the courts and the applicable law regarding crowdworking.

Key Words: Crowdwork, Characterization, Independent Contractors, International Jurisdiction, Applicable Law

1. Introduction

As a result of the developments in information and communication technologies (ICT) in the 21st century, digital economy has gained more importance. The digital economy is transforming societies and changing socio-economic relations.¹ In other words, the work organization and the relationship between employer and employee are altering dimensions. Especially with the COVID-19 pandemic, people started working from home instead of going to their offices and as a result, remote working became widespread.²

Digital work platforms offer new forms of informal employment whose attractiveness is mainly based on the possibility of obtaining freely performed paid work. More specifically, these platforms offer online intermediation services, which essentially consist of connecting clients and service providers. One category of platform work consists of tasks that take place in the real world and are powered by a website or app, such as Uber³ (ridesharing) and Glovo⁴

1 Valerio De Stefano and Antonio Aloisi, ‘European Legal Framework for “Digital Labour Platforms”’, (2018), European Commission, Luxembourg, 2.

2 Uglješa Grušić, ‘Remote working and European private international law’ (2022) ETUI Research Paper – Policy Brief 2022/09, 2 <<https://www.etui.org/sites/default/files/2022-12/Remote%20working%20and%20European%20private%20international%20law-2022.pdf>> accessed 30 May 2024.

3 Uber, American international transportation network company based in San Francisco, California, connects the physical and digital worlds to help make movement happen at the touch of a button. In addition to the transport service, it is committed to providing services that individuals need, such as meal delivery and delivery of prescription medicines: Uber, About us, <<https://www.uber.com/hr/en/about/>> accessed 4 April 2023.

4 Glovo is a Spanish-based company that has developed a technology that connects customers with local businesses through a large network of couriers who have signed up to offer delivery services: Glovo, This is Glovo, <<https://about.glovoapp.com/this-is-glovo/>>, accessed 4 April 2023.

(food delivery)⁵. The other category, represented by Upwork⁶ or by Amazon's Mechanical Turk⁷ (MTurk), involve completion of computer tasks online.⁸ In other words, the services offered via these platforms are performed entirely online like translate, graphic design, computer programming and data-entry tasks.

Digital work platforms are part of a new form of *sharing economy* or *on-demand economy* or *gig economy* bringing together all the digital platforms that make it possible to connect suppliers and demandants for goods or services via the internet.⁹ Service providers offering their services through the platforms are attracted by the possibility of working remotely as well as by the flexibility in time, space and organisation of this form of work. However, these advantages are opposed by the disadvantages which are essentially linked to the lack of stability, low remuneration and reduced access to social protection. The extent of these risks, however, depends on the intensity of the use of platform intermediation services to obtain paid work.¹⁰ While it is true that some people focus their professional activity on digital work platforms, most providers only use their services on an *ad hoc* basis to supplement another source of income.

In this tripartite relationship brought about by digital economy, qualification is important in terms of determining the rights and obligations of the parties. Especially in disputes with an international element, qualification is essential for determining the applicable law and the international jurisdiction of the courts. The issue of whether the relationship between the platform and the service provider is an employment relationship has not yet been established on a legal basis. Most digital work platforms do not view themselves as an employer but as an entity or rather a system, whose role is limited to establishing the connection between the client and the service provider. The general conditions of the platforms specify, most of the time, that the service-provider is self-employed. Platform workers gain guaranteed rest time and paid holidays, at least the national or sectoral minimum wage (where applicable), safety and health protection, unemployment, sickness and health care benefits, maternity, paternity and parental leave, pension rights, benefits relating to accidents at work

5 Miriam A Cherry, Regulatory Options for Conflicts of Law and Jurisdictional Issues in the on-demand Economy (International Labour Organization 2019), 7.

6 Upwork Global Inc., formerly Elance-oDesk, is an American freelancing platform based in Santa Clara and San Francisco, California, <<https://www.upwork.com/about>>, accessed 5 April 2023.

7 Amazon Mechanical Turk is a crowdsourcing marketplace enabling individuals and businesses (known as Requesters) to engage a 24/7, global distributed workforce (known as Workers) to perform tasks, <<https://www.mturk.com/product-details>>, accessed 5 April 2023.

8 Cherry, 'Regulatory Options' (n 5), 7.

9 Florence Guillaume, 'Le Contrat de Travail International: Règles de Droit International Privé et Plateformes Numériques', in Dunand Jean-Philippe and Mahon Pascal (eds), *Les aspects internationaux du droit du travail* (Schulthess 2019), 227.

10 Guillaume (n 9), 228.

and occupational diseases from being classified as employees.¹¹ Therefore, the nature of the relationship between the service providers and the platform has been the subject of debate in many cases.

2. International element

The relation between platforms and their service providers is, most of the time, international or potentially international.¹² The platforms offering services in the real world have a more localized field of activity contrary to the platforms offering services completely online. For example, an Uber driver physically performs their service by picking up a passenger from a specific geographical location and dropping them off in a specific geographical area. The relationship between the platform and the service provider is an international one, in any case, when the domicile of the persons or of the company managing and maintaining the platform is in a State other than that of the domicile of the service provider, or when the latter must execute their performance in a State other than that of their domicile.

With regard to platforms offering services entirely online, they are generally aimed at service providers located anywhere. On the internet, which is independent of the real world,¹³ it is difficult to identify the international element.¹⁴ Transactions on the internet have an international element as they have the potential to have an impact in more than one country or around the globe, or are more likely to have an international element.¹⁵ In other words, the internet, which is referred to as the network of networks, inherently contains an international element.¹⁶ However, automatically recognizing every transaction that takes place on the internet as having an international element may not always lead to the right results. For example, an agreement for an online service between citizens of the country on which the platform is based cannot be

11 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'The European Pillar of Social Rights Action Plan', COM(2021) 102 final.

12 Guillaume (n 9), 232.

13 See about the characteristics of the internet Tobias Lutz, 'Internet Cases in EU Private International Law: Developing A Coherent Approach' (2017) 66 ICLQ 687, 688.

14 Obdulio César Velásquez Posada, 'Jurisdictional Problems in Cyberspace Defamation' (2005) *International Law: Revista Colombiana de Derecho Internacional*, 6, 258.

15 Axel Nilsson, *Personality Rights, Defamation and the Internet*, Lund University Faculty of Law, Graduate Thesis Master of Laws Program, Sweden 2017, 19.

16 Catherine Kessedjian, 'Rapport de Synthèse' in Katharina Boele-Woelki and Catherine Kessedjian (eds), *Internet Which Court Decides? Which Law Applies? Quel Tribunal Décide? Quel Droit s' Applique?* (Kluwer 1998), 143-144; Tristan Azzi, 'Atteintes en Ligne aux Droits de la Personnalité et aux Droits de Propriété Intellectuelle: Tribunal Compétent et Loi Applicable' (2014) 52 *Legicom: Revue Thématique de Droit de la Communication* 39.

considered international just because it takes place online. Each employment relationship performed on the internet must be evaluated case by case as a result of this evaluation, whereby the existence of the international element must be concluded.

3. Characterisation

Characterisation is a crucial step to accommodate the facts within legal categories.¹⁷ The characterisation of the relationship between the platform and its service providers is not only useful to establish whether the protective standards of labour law can be invoked, but also to determine which rules of private international law apply.¹⁸ Therefore, the nature of the relationship between the service provider and the platform should be clarified in order to determine international jurisdiction of courts and the applicable law.

It is necessary to determine whether the relationship between the service provider and the platform is an employment relationship, both for the protective standards arising from labour law and to determine the applicable law in private international law.¹⁹ The issue of whether platform workers are employees or independent contractors has been debated in many jurisdictions.²⁰ The platforms have been accused of misclassifying their service providers as *independent contractors* to avoid labour law obligations.²¹ The lack of homogeneity between the platforms makes it difficult to unify decisions about characterisation.²²

Some platform workers, like employees, often have limited control over their work (eg in some cases they cannot set prices, must wear uniforms, cannot choose the order of their tasks) and/or are dependent on their clients/employers in other ways (eg financially).²³ This control can be implemented through technology-assisted monitoring with the algorithm replacing a traditional manager.²⁴ For example, Uber has been reported to monitor the smartphones of

17 Reflecting Savigny's influence on private international law, the characterization seeks to identify the seat (Sitz) of the facts: Geert van Calster, *European Private International Law*, (2nd edn, Hart Publishing, 2016), 6.

18 Guillaume (n 9), 231.

19 Ilaria Pretelli, 'Protecting Digital Platform Users by Means of Private International Law' (2021) 13 Cuadernos de Derecho Transnacional 574, 581.

20 Some EU jurisdictions have a third category of 'dependent contractor' or 'self-employed worker', which can make classification lawsuits even more complicated.

21 Asger Lund-Sorensen, 'Jurisdictional Clauses in Platform Work Contracts: A Danish Perspective' (2018) 1 Nordic Journal of Commercial Law 261, 265.

22 Guillaume (n 9), 229.

23 Marguerita Lane, 'Regulating platform work in the digital age' (OECD 2020) <<https://goingdigital.oecd.org/toolkitnotes/regulating-platform-work-in-the-digital-age.pdf>>, accessed 30 May 2024, 7.

24 Lane (n 23), 7.

its drivers to map how they were using the pedals and identify good and bad acceleration and braking practices.²⁵ Platforms have different technical structures and subordination between the platform and its workers also varies from platform to platform. Therefore, the characterisation must be made on a case-by-case basis,²⁶ depending on the characteristics of the platform in question.²⁷

3.1. Characterisation in the United States

Cases concerning platform work have been the subject of intense debate in the US, where common law is dominant, and a number of criteria have been developed.²⁸ In this context, the right to control test and the ABC test should be mentioned.

In American Law, the Fair Labor Standards Act regulating minimum wage and overtime pay defines ‘employee’ as an individual employed by an employer and defines ‘employ’ as to offer or permit to work.²⁹ According to this test, in order to determine whether a person is an employee or not, the degree of control exercised by the presumed employer over the performance of the work is taken into account.³⁰ This test analyses the following factors:

1. Whether the person performing services is engaged in an occupation or business distinct from that of the principal;
2. Whether or not the work is a part of the regular business of the principal or alleged employer;
3. Whether the principal or the worker supplies the instrumentalities, tools, and the place for the person doing the work;
4. The alleged employee’s investment in the equipment or materials required by their task or their employment of helpers;
5. Whether the service rendered requires a special skill;

25 Antonio Aloisi and Valerio de Stefano, *Your Boss is an Algorithm* (1st edn, Hart Publishing 2022), 59.

26 Kamila Naumowicz, ‘Some Remarks to the Legal Status of Platform Workers in the Light of the Latest European Jurisprudence’ (2021) 28 *Studia z Zakresu Prawa Pracy i Polityki Społecznej* 177, 183.

27 Guillaume (n 9), 234.

28 Within the scope of our study, the law of the United States of America is only addressed in the characterisation section. The section on applicable law and jurisdiction will only include explanations according to the European Union Regulations.

29 1. 29 U.S.C. § 203(e)(1), (g) (2006); see also Alek Felstiner, ‘Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry’ (2011) 32 *Berkeley Journal of Employment and Labor Law* 143 169; Gaye Baycık, Orhan Ersun Civan, Hazal Tolu Yılmaz, Berrin Bosna, ‘Platform Çalışanlarını Yasal Güvenceye Kavuşturmak: Sorunlar ve Çözüm Önerileri’ (2021) *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi* 713, 748.

30 Carissa Laughlin, ‘Arbitration Clause Issues in Sharing Economy Contracts’ (2017) *Journal of Dispute Resolution* 197, 203; Hazal Tolu Yılmaz, *İş ve Sosyal Güvenlik Hukuku Bakımından Dijital Platform Çalışanlarının Hukuki Statüsü*, Galatasaray University Graduate School of Social Sciences, PhD Thesis, İstanbul 2022, 98.

6. The kind of occupation, with reference to whether, in the locality, the work is usually done under the direction of the principal or by a specialist without supervision;

7. The alleged employee's opportunity for profit or loss depending on his or her managerial skill;

8. The length of time for which the services are to be performed;

9. The degree of permanence of the working relationship;

10. The method of payment, whether by time or by the job; and

11. Whether or not the parties believe they are creating an employer-employee relationship;

12. Last but not least, whether the person to whom service is rendered (the employer or principal) has control or the right to control the worker both as to the work done and the manner and means in which it is performed.³¹

The California Supreme Court's decision on *Dynamex Operations West, Inc. v. Superior Court*³² was based on the ABC test which states that a business wishing to classify workers as independent contractors must satisfy three elements:³³

A) that the worker is free from the control and direction of the hirer in connection with the performance of work, both under the contract for the performance of such work and in fact;

B) that the worker performs work that is outside the usual course of the hiring entity's business; and

C) that the worker is customarily engaged in an independently established trade, occupation, or business of the same nature as the work performed for the hiring entity.³⁴

With the *Dynamex* case, the employer has the burden of proving that a person that works for them is not an employee.

3.2. Characterisation in Europe

In EU the essential feature of an employment relationship is that a person, for a certain period of time, performs services for and under the direction of another, in return for which remuneration is paid.³⁵ The EU law does not set

31 Kieran Van Den Bergh, 'United States' in Isabelle Daugareilh, Christophe Degryse and Philippe Pochet (eds), *The Platform Economy and Social Law: Key Issues in Comparative Perspective* (Working Paper, 2019.10), 130.

32 *Dynamex Operations W. v. Superior Court*, 4 Cal.5th 903 (2018).

33 Cherry 'Regulatory Options' (n 5),19; *Dynamex Operations W.* (n. 32); Christina Hiebl, 'The Legal Status of Platform Workers: Regulatory Approaches and Prospects of A European Solution' (2022) 15 Italian Labour Law E-Journal, <<https://illeg.unibo.it/article/view/15210>>, accessed 18 April 2023, 14-15.

34 *Dynamex Operations W.* (n. 32)

35 Case C-232/09 *Dita Danosa v LKB Lixings SLA* [2010] ECR I-11405, para 39.

additional conditions like the existence of a formal contract between the employee and the employer.³⁶

In *Aslam v Uber*,³⁷ the London Employment Tribunal held that the Uber drivers who brought the case were ‘workers’, an intermediate status between employee and independent contractor.³⁸ The Tribunal stated that Uber had imposed a great number of conditions on the drivers, managed and instructed the drivers through the cellphone app, and overall, controlled the drivers’ working conditions³⁹.

In Belgium, the Administrative Commission for the Governance of the Employment Relationship decided that Deliveroo food-delivery bicycle riders were employees under Belgian law.⁴⁰ The Commission stated that Deliveroo riders do not control their working time, since they must reserve their work slots more than one week in advance.⁴¹

The German Federal Labor Court (Bundesarbeitsgericht) ruled, on 1 December 2020, that a person working on a location-based platform is an employee.⁴² In the case in dispute, the claimant controls how retail products belonging to users are presented to customers.⁴³ The claimant goes to the store where the product is offered, takes photographs of the product and answers questions about it. Employees according to the platform’s operating model, have the option to accept or reject the work assigned to them, and the accepted work must be completed in two hours. Employees receive both wages and experience points for the tasks they complete on the platform and as experience points accumulate, employees’ status on the platform becomes stronger. This allows employees to be assigned to more tasks which in turn incentivizes employees to accept more work. The claimant worked an average of 20 hours per week for a period of 11 months, earning a monthly income of approximately 1750 euros. The fact that the employee is obliged to complete the work within two hours and that the manner in which the work is to be performed is

36 Uglješa Grušić, *The European Private International Law of Employment* (1st edn, CUP 2015), 79.

37 [2016] EW Misc B68, [97] (ET) (28 Oct. 2016); Nikola Countouris, ‘Regulatory and Jurisprudential Perspectives on Platform Work: The UK Case’ in Maria Teresa Carinci and Filip Dorssemont (eds), *Platform Work in Europe Towards Harmonisation?* (Intersentia 2021), 157.

38 Cherry ‘Regulatory Options’ (n 5), 20.

39 *ibid.*, 20-21; Countouris, 157-158.

40 *ibid.*, 21; Commission Administrative de règlement de la relation de travail (CRT) Feb. 23, 2018, No. 116-FR-20180209; Fabienne Kéfer, ‘Platform Work: The Belgian Case’ in Maria Teresa Carinci and Filip Dorssemont (eds), (n 37), 9-10.

41 Cherry ‘Regulatory Options’ (n 5), 21.

42 BAG, 01.12.2020 - 9 AZR 102/20; Tolu Yılmaz (n 30), 94; Gerrard Boot, ‘Platform Work in Europe: The Need for a Multilevel Solution to Protect the So-Called Self-Employed’ (2022) 13 European Labour Law Journal 81, 82.

43 Rüdiger Krause, ‘App-Based’ Work: The German Case’ in Maria Teresa Carinci and Filip Dorssemont (eds) (n 37), 37-41.

determined in detail and communicated to the employee proves the subordination. In this decision, platforms' incentive systems that influence the will of employees are accepted as an indicator of subordination.

Since there is no uniformity regarding the status of platform employees, even the courts of the same country can render different judgments on this issue. Hence, our statements hereinafter will be based on the assumption that platform workers are employees.

4. International jurisdiction

If we consider these service providers as employees, how will we appoint the competent court? One of the most important problems in cross-border proceedings is the determination of the competent court. The European rules on international jurisdiction are unified by Brussels I-bis Regulation.⁴⁴ Its system and many of its provisions date back to its predecessor, the Brussels Convention.⁴⁵ This regulation contains various protective provisions in favor of the party that does not have equal bargaining power in employment, consumer and insurance contracts.⁴⁶

Brussels I-bis Regulation has a special section (n. 5) about jurisdiction over individual employment contract. The provisions aimed at protecting the position of a weaker party in litigation under the Brussels I-bis regime can be summarised as follows:

a) A weaker party (an employee) has a choice to bring proceedings against the other party to a contract either in the court of the Member State in which that other party is domiciled or in which it is more convenient to a weaker party (most likely in the country of its own domicile) or which is otherwise closely related to the dispute.

b) Conversely, proceedings may be brought against a weaker party to the contract only in the courts of the Member State in which the 'weaker' party is domiciled.

c) Forum choice clauses in these disputes have limited binding effect against a 'weaker' party. They may be successfully invoked against a weaker party only if the conditions provided in the relevant provisions of the Regulation are met.⁴⁷

44 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L 351/1 and subsequent amendments.

45 Convention on jurisdiction and the enforcement of judgments in civil and commercial matters (Brussels, 27 September 1968) [1972] OJ L 299/32.

46 Recital 18 in the preamble to Brussels I-bis Regulation. See also Vesna Lazić, 'Procedural Position of a "Weaker Party" in the Regulation Brussels Ibis' in Vesna Lazić and Steven Stuij (eds), *Short Studies in Private International Law* (Springer 2017), 52; Van Calster (n 17), 29, footnote 36; Grušić, *The European Private* (n 36), 7.

47 Lazić, 53.

4.1. Jurisdiction agreements

Allowing the parties to choose the jurisdiction creates legal certainty and predictability and party autonomy is therefore of paramount importance in private international law.⁴⁸ Brussels I-bis Regulation also permits, in principle, jurisdictional agreements to achieve these objectives.⁴⁹ Within this scope art 25 of Brussel I-bis Regulation gives the parties the possibility of agreeing on jurisdiction of the courts of Member States. Pursuant to art 23 of Brussels I-bis Regulation, a jurisdiction agreement will be given effect in an employment dispute only if it is entered into after the dispute has arisen or if it allows the employee to bring proceedings in courts other than those indicated by the default rules.⁵⁰

Platforms frequently include jurisdiction and arbitration⁵¹ agreements in their general terms and conditions. The general conditions of the platforms are presented on the basis of ‘take it or leave it’.⁵² In other words, platform users do not have the right to negotiate these terms. These general terms and conditions are very long and dense and contain a lot of legalese.⁵³ Since platform work often involves an international element, especially when the work is performed online, employees are forced to accept these general terms and conditions without bargaining, which are not mostly in the language that they can speak. The Brussels I-bis Regulation specifically regulates jurisdiction agreements in employment contracts in order to protect the weaker party and only allows jurisdiction agreements in limited circumstances.

4.2. Rules on Jurisdiction of Brussel I-bis Regulation

Brussels I-bis Regulation gives employees access to more forums than employers.⁵⁴ When the employer is the claimant, an employee domiciled in a Member State may be sued only *in the courts of the employee’s domicile* but when the employee is the claimant, an employer domiciled in a Member State may be sued: in the courts of the employer’s domicile; in the courts of the place where or from where the employee habitually carries out his/her work (or in the

48 Lund-Sørensen (n 21), 267.

49 Recital 19 of the preamble of Brussels I bis Regulation reads as follows, ‘The autonomy of the parties to a contract, other than an insurance, consumer or employment contract, where only limited autonomy to determine the courts having jurisdiction is allowed, should be respected subject to the exclusive grounds of jurisdiction laid down in this Regulation’.

50 Grušić, *The European Private* (n 36), 126-127.

51 It should be noted that arbitration agreements regarding platform work are outside the scope of this study but for detailed information on the subject see Laughlin, 196-217.

52 Lund-Sørensen (n 21), 268.

53 Cherry ‘Regulatory Options’ (n 5), 25.

54 Grušić, ‘Remote Working’ (n 2), 3.

courts for the last place where he did so); if there is no habitual place of work, in the courts of the engaging place of business.

For example an employer who is domiciled in Belgium hires an employee who is domiciled in Croatia and habitually carries out their work in Croatia, can sue the employee only in Croatia while the employee may bring proceedings in either Belgium and Croatia. The rules in the Brussels I-bis Regulation are clear, but it is necessary to clarify what we should understand by habitual place of work. Where work is carried out at a single location, the habitual place of work can be easily identified.⁵⁵ In the case of peripatetic work, work carried out in more than one jurisdiction, it will be difficult to determine the habitual place of work.⁵⁶ The Court of Justice of the European Union (CJEU) has issued several decisions⁵⁷ to determine the habitual place of work for this type of work. The long and the short of the matter, the term ‘habitual place of work’ is effectively equivalued with ‘principal place of employment’.⁵⁸ In these decisions, the CJEU has taken into account the duration of the employee’s employment and whether the employee has an office in a country. However the term is interpreted widely in that the determination of the habitual place of work is essentially a search for the place that is most closely connected with the employment dispute.⁵⁹

55 Grušić, *The European Private* (n 36), 110.

56 In this context, digital nomads can also be mentioned. Digital nomads are professionals who perform work digitally over the internet to have a lifestyle of constant travelling or expat living. In this digital era the digital nomad lifestyle is attracting people. Some Countries are creating special visas for these new type of employees. For example Estonia is about to give visa for digital nomads allowing workers living temporarily in Estonia to have the right to reside there for 365 days while benefitting from a Schengen visa, Guillaume (n 9), 240–241 footnote 168; see also Ekaterina Chevtava and Basak Denizci-Guillet, ‘Digital Nomads’ Lifestyles and Coworkation’ (2021) 21 *Journal of Destination Marketing and Management* 1, <<https://www.sciencedirect.com/science/article/abs/pii/S2212571X21000810>> accessed 10 April 2023; Hannonen Olga, ‘In Search of a Digital Nomad: Defining the Phenomenon’ (2020) 22 *Information, Technology and Tourism* 335, 336. ‘To maintain their lifestyle while constantly traveling the world, digital nomads engage with works that create digital goods using digital tools, Caleece Nash, Mohammad Hossein Jarrahi, Will Sutherland and Gabriela Phillips, ‘Digital Nomads Beyond the Buzzword: Defining Digital Nomadic Work and Use of Digital Technologies’ in Gobinda Chowdhury, Julie McLeod, Val Gillet and Peter Willett (eds), *iConference 2018: Transforming Digital Worlds* (Springer 2018), 209.

57 Case C-125/92 *Mulox IBC Ltd v Geels* [1995] ECR I-04075; Case C-383/95 *Rutten v Cross Medical Ltd.* [1997] ECR I-00057; Case C-37/00 *Weber v Universal Ogden Services Ltd.* [2002] ECR I-02013; Joined Cases C-168/16 and C-169/16 *Sandra Nogueira v Crewlink Ireland Ltd and Moreno Oscar v Ryanair* [2017] ECLI:EU:C:2017:688. For a detailed assessment of the decisions see Grušić, *The European Private* (n 36), 109–115.

58 Grušić, *The European Private* (n 36), 114.

59 *ibid.*

5. Applicable law

Rome I Regulation⁶⁰ determines the law applicable to individual employment contracts. As in the Brussels I-bis Regulation, the Rome I Regulation also includes provisions protecting the weaker party.⁶¹ Recital 23 of the preamble of Rome I Regulation reads as follows, '[a]s regards contracts concluded with parties regarded as being weaker, those parties should be protected by conflict of law rules that are more favourable to their interests than the general rules'.

5.1. Choice of the Law Applicable to the Individual Employment Contract

Since the technique of geographical localisation encounters limits in the environment of digital work platforms, it is necessary to check whether a subjective criterion, based on the autonomy of the parties, is likely to improve legal security. In some legal systems, party autonomy is completely prohibited or limited, while in others it is accepted provided that it is in compliance with mandatory rules or public policy.⁶² In EU private international law employees are recognized to have less bargaining power, and the concern is that choice of law provisions might not work to their advantage.⁶³ Rome I Regulation seeks to set a 'minimum standard of employment protection that cannot be undermined by the chosen law'.⁶⁴

According to art 3 of the Rome I Regulation,

A contract shall be governed by the law chosen by the parties. The choice shall be made expressly or clearly demonstrated by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or to part only of the contract.

However, art 8 of Rome I Regulation on individual employment contracts sets minimum standards for the validity of this choice.

According to art 8(1) of Rome I Regulation,

An individual employment contract shall be governed by the law chosen by the parties in accordance with Article 3. Such a choice of law may not, however, have the result of depriving the employee of the protection afforded to him by provisions that cannot be derogated from by agreement under the law that, in the

60 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations, [2008] OJ L 177.

61 On the reasons underlying the protection of the employee see Maria Campo Comba, *The Law Applicable to Cross-Border Contracts Involving Weaker Parties in EU Private International Law* (1st edn, Springer 2021), 30–33.

62 Grušić, *The European Private* (n 36), 39.

63 Miriam A. Cherry, 'A Global System of Work, A Global System of Regulation?: Crowdwork and Conflicts of Law' (2019) 94 *Tulane Law Review* 1.

64 Cherry, 'A Global System of Work' (n 63), 37.

absence of choice, would have been applicable pursuant to paragraphs 2, 3 and 4 of this Article.

Therefore a limited choice of law is allowed in individual employment contracts.⁶⁵ In other words, when parties have chosen the law applicable to their employment contract, the judge must firstly determine which law would be objectively applicable according to the following paragraphs of article 8 of Rome I Regulation and afterwards compare that law to the chosen law to conclude whether the chosen law offers the same or a better protection to the employee than the mandatory provisions of the objectively applicable law.⁶⁶

The general terms and conditions of the platforms provide, almost systematically, for choice of law clauses designating the applicable law in the State where the registered office of the company that manages and maintains the platform. However these general terms of service are drafted by the legal advisors of the platforms, and they primarily take into account the interests of the platforms. The service provider will often have to accept these non-negotiable terms and conditions in order to become a part of the platform. Thus, it is necessary to determine the relevant mandatory provisions for pending action and then compare which ones offer a better protection to the employee.

5.2. Objective Connecting Factors: The Law Applicable in the Absence of Choice

When the parties have not chosen the law applicable to their contract, the law applicable to the individual employment contract will be designated by the conflict rules contained in paragraphs 2, 3 and 4 of art 8 Rome I Regulation. According to these paragraphs,

(2) To the extent that the law applicable to the individual employment contract has not been chosen by the parties, the contract shall be governed by the law of the country in which or, failing that, from which the employee habitually carries out his work in performance of the contract. The country where the work is habitually carried out shall not be deemed to have changed if he is temporarily employed in another country.

(3) Where the law applicable cannot be determined pursuant to paragraph 2, the contract shall be governed by the law of the country where the place of business through which the employee was engaged is situated.

(4) Where it appears from the circumstances as a whole that the contract is more closely connected with a country other than that indicated in paragraphs 2 or 3, the law of that other country shall apply.

⁶⁵ Campo Comba (n 61), 119.

⁶⁶ *ibid.*

As it is understood from the provision, geographical connections such as the habitual place of work and the engaging place of business determine the applicable law.

6. Localisation using traditional rules

The classic connecting method of private international law aims to determine the seat (*le siège*) of the legal relationship in question.⁶⁷ The objective is, therefore, to localize the legal relationship in a space, within the borders of a State. We have mentioned local connections such as habitual place of work in the explanations on both international jurisdiction and applicable law. However, it will be extremely difficult to locate a transaction carried out in the digital space of the internet in a physical space.

In this context, we need to create a dichotomy. It will undoubtedly not be the same case in platform work models where the work takes place entirely online and where the work takes place in a physical environment. Indeed it is easier to localize work that takes place in a physical environment according to these rules than work that takes place entirely on the internet. The service is generally performed in the presence of the service provider and the client. For example, the driver picks up the customer and takes them from one place to another. In this context, the use of the internet only facilitates the linking of the various parties and has no significant impact on the application of the rules of private international law.⁶⁸

On the other hand, there are platforms like Upwork, where localization is a big problem, where the service takes place entirely on the internet. When the work is performed online, the habitual place of work means the location of worker with their computer connected to the internet⁶⁹. However, online work is not necessarily carried out on the territory of a single State. Crowdworkers may work from any location. For digital nomads the service can be carried out in several different countries during a trip, which makes any localisation to the habitual link impossible. Besides, the service provider generally performs several successive performances for the platform. If it must be concluded from all of these services that it is not possible to determine the center of gravity of the worker's activity, the other connecting criteria such as the place of domicile or habitual residence of worker, the place where the establishment, domicile or habitual residence of the employer is located must apply.⁷⁰ The location of the employee's domicile or habitual residence will not always be easy in practice (in

67 Guillaume (n 9), 239.

68 *ibid*, 240.

69 *ibid*.

70 *ibid*, 241.

the example of digital nomads). It is doubtful that protective function of rules on international jurisdiction and applicable law is fulfilled when the employee has an itinerant lifestyle.

To sum up, the traditional connecting factors are therefore very difficult to apply when the service is provided entirely online. Even the possibility that the employee fictively determines the place of the performance takes place in the contract will not solve the problem. It would be preferable to recognize that this type of legal relationship takes place in a digital environment that is disconnected from any territorial link, while seeking another means of determining the forum and the applicable law.⁷¹

7. As a conclusion: some solutions

Crowdwork, which is the product of the technological age, has raised various problems in both substantive law and private international law. Especially transactions on platforms where the entire service takes place on the internet, often have an international element and therefore fall within the scope of private international law. In the crowdwork, where there is a tripartite relationship, it is important to characterize the relationship between the service provider and the platform. If the service provider is characterized as an employee in this relationship, the protective measures arising from labour law will also apply to the service provider. Moreover, the platforms have been accused of misclassifying their service providers as independent contractors to avoid labour law obligations. Characterization is therefore very important, but it is difficult to draw general conclusions as the technical characteristics of the platforms differ from one another. However, there is no uniformity regarding the status of platform employees, even the courts of same country can render different judgments on this issue.

The status of platform workers is a grey area in private international law. Assuming that these service providers are employees, they will be subject to the Brussels I-bis and Rome I Regulations. These regulations, which are related to international jurisdiction and applicable law respectively, contain provisions protecting the employee, who is considered to be the weaker party. These Regulations also include geographical connecting factors such as the employee's habitual place of work but on platforms like Upwork, where the work takes place only on the internet, using these geographical connecting factors undermines predictability. Especially in the case of digital nomads, these geographical connecting factors may point to incidental locations and may not fulfill the objective of protecting the weaker party. Therefore, it is difficult to apply the

⁷¹ *ibid*, 243.

classical conflict of laws rules to these employees. Even the characterization has not been established on a clear basis yet.

According to a solution argued in the doctrine, these employees should be protected sectorally such as seafarers which have fallen outside and apart from the territorial jurisdiction of national regulation.⁷² As a matter of fact, these platforms do not harm the labour market, and these platforms increase job opportunities. Ensuring predictability and legal security to platforms and granting legal status to employees will be in favor of the labour market.⁷³ According to another proposal, online dispute resolution (ODR) methods should be provided for these disputes.⁷⁴ The objective of this online dispute resolution platform is to provide a simple, effective, fast and inexpensive out-of-court solution to disputes arising from online transactions. An online dispute resolution system would also be attractive for digital employees who are often discouraged from submitting their low-value claims to judges or arbitrators.

72 Cherry (n 66), 50.

73 Baycık and others (n 29), 791.

74 Guillaume (n 9), 254.

The Potential of Digital Markets Act and Digital Services Act to Provide a Meaningful Legal Framework for Collaborative Economy Platforms in the EU

Wojciech Lewandowski *

Institute of Law Studies Polish Academy of Sciences

ORCID 0000-0002-3909-6519

DOI: 10.54103/milanoup.215.c453

Abstract

Collaborative economy platforms (such as Uber or Airbnb) have been in the past under scrutiny by the Court of Justice of the EU under the framework of the Services Directive. With the conclusion of the rulings in Uber and Airbnb cases that their activities remain outside of the scope of this legislation. Simultaneously, the former E-Commerce Directive might not provide solutions adapted to the innovative models of peer-to-peer platforms and services. Hence, a legal vacuum might materialize in which the activity of the operators of the collaborative economy platforms on the Internal Market would remain outside the scope of the EU law. Digital Markets Act and Digital Services Act entered into force in November 2022. The new EU legislation was intended to introduce responsibility requirements for platform operators, regulate the activity of ‘gatekeepers’ and will provide the legal framework for the operation of the biggest digital platforms in the Internal Market. The question emerges – to what extent this regulation would provide a meaningful legal framework for the activity of collaborative economy platforms in the Internal Market? The ambition of the submitted contribution would be to respond to this question based on the analysis of the adopted provisions of the DSA and DMA. For this purpose, the systemic review of the existing literature on the regulating of collaborative economy platforms will be conducted. The analysis will also refer to the jurisprudence of the Court of Justice on the scope of application of the Services Directive and E-Commerce Directive in the context of the activity of

* The contribution was funded by the National Science Centre, Poland under the project with registry No. 2017/27/B/HS5/02073.

Uber and Airbnb. Thirdly, the author will also assess the approach of the EU institutions to the collaborative economy platforms (exemplified by the above-mentioned rulings and legislation, as well as the European Commission's policy documents) in the context of regulating the activity of transnational entities. The main argument of the paper will be based on the assumption that the lack of a meaningful legal framework for the economic activity of the collaborative economy platforms might lead to the deterioration of the protection of the economic interests of the users of these platforms. The second argument of the paper, building on the main one, suggests that such an outcome would be evidence of a non-interventionist policy of the EU and a lenient approach of the EU towards collaborative economy platforms. These arguments will be critically assessed and verified with the results of the analysis of the potential of the DSA and DMA to regulate their activities in line with the other types of digital platforms and 'gatekeepers'.

Keywords

Digital Services Act, Digital Markets Act, Sharing Economy, Freedom of Services, Internal Market

1. Introduction

Legal challenges related to the activities of collaborative economy platforms have been the subject of many studies in the literature in the past¹ and more recently². It has also been a subject of increased activity of the European Commission back in 2016-2018 which resulted in the publishing of several economic studies on the collaborative economy³ and led to the adoption of the soft-law policy document – the communication 'A European agenda for the collaborative economy' (the 'Collaborative Economy Communication')⁴. One of the main challenges related to the presence of new, innovative, and disruptive business models pursued by the collaborative economy platforms was the identification of a suitable and meaningful legal framework for their

1 V Hatzopoulos, *The Collaborative Economy and EU Law* (Hart Publishing 2018) see also: N M Davidson, M Finck, JM Infranca (eds), *The Cambridge Handbook of The Law of the Sharing Economy* (CUP, 2018).

2 For comprehensive analysis see: Vida Česnuitytė and others, *The sharing economy in Europe: Developments, practices and contradictions* (Cham: Palgrave MacMillan 2022).

3 Commission, Directorate General for Internal Market, Industry, Entrepreneurship and SMEs, 'Collaborative economy studies' (2018) <https://single-market-economy.ec.europa.eu/single-market/services/collaborative-economy/collaborative-economy-studies_en> accessed 7 May 2023.

4 Commission, 'A European agenda for the collaborative economy' (Communication), COM (2016) 356 final.

operations⁵. The main two fields of research have been competition law⁶ and freedom to provide services⁷. The Commission described it in the Collaborative Economy Communication in the following manner:

The collaborative economy often raises issues with regard to the application of existing legal frameworks, blurring established lines between consumer and provider, employee and self-employed, or the professional and non-professional provision of services. This can result in uncertainty over applicable rules, especially when combined with regulatory fragmentation stemming from divergent regulatory approaches at national or local level. This hampers the development of the collaborative economy in Europe and prevents its benefits to materialise fully. At the same time, there is a risk that regulatory grey zones are exploited to circumvent rules designed to preserve the public interest.

Hence, the ambition of this contribution is to analyse whether the challenges identified by the Commission have been resolved since the adoption of Collaborative Economy Communication. For this purpose, the contribution was divided into 4 main sections. The first issue that is discussed in Section 2 was related to the struggles with the legal classification of the activities of collaborative economy platforms and the attempt to identify suitable definitions in existing and recently adopted EU legislation. The scope was limited to the *eCommerce* Directive, Services Directive, Digital Services Act (DSA), and Digital Markets Act (DMA).⁸ The legal definition allows us to determine the scope of requirements and obligations stemming from the EU law, as well as draw the line between the competencies field of the EU and Member States. For better clarity, these topics were presented in Section 3 and Section 4. Section 3 focused on the established framework and interpretation provided by the Court of Justice of the European Union in its jurisprudence. Section 4 assesses the potential obligations of DSA and DMA in the context of the scope of application of these new legal acts. Section 5 discusses the outcomes of these analyses against the background of the EU digital policy and the approach towards transnational private platforms. The impacts of the policy of the EU towards collaborative economy platforms (embodied by the applicable legislation, suitable legal framework, policy documents of the Commission, and jurisprudence

5 K Erickson and I Sørensen, 'Regulating the sharing economy', (2016) 5/2 Internet Policy Review, <<https://doi.org/10.14763/2016.2.414>> accessed 30 April 2023.

6 G Lougher and S Kalmanowicz, 'EU Competition Law in the Sharing Economy', (2016) 7/2 Journal of European Competition Law & Practice, S P King, 'Sharing Economy: What Challenges for Competition Law?', (2015) 6/10 Journal of European Competition Law & Practice. See also: MD Iacob, 'Collaborative economy - regulations at European Union level and its impact on the competitive environment', [2017] Romanian Competition Journal.

7 C Cauffman and J M Smits, (2016), 'The Sharing Economy and the Law: Food for European Lawyers', (2016) 23/6 Maastricht Journal of European and Comparative Law.

8 See *infra* respectively (n 11), (n 19), (n 20), (n 21).

of the Court) are discussed in the context of the competitiveness of the EU and the protection of the users. A summary of the main conclusion is presented in Section 6.

2. Definition of collaborative economy platforms

To assess the compatibility of existing legal frameworks to the activities of collaborative economy platforms in the Internal Market it is necessary to determine the definition for these kinds of entities. The definition will allow them to classify their activities and potentially apply the provisions of the EU law to many different factual situations related to their activities in different sectors of the economy. The lack of an EU-wide uniform definition applicable across different sectors and jurisdictions might lead to the fragmentation of the Internal Market⁹. Thus, to determine the existence of a union-level definition, the main policy documents published by the European Commission were analysed, as well as the 4 legal acts analysed in this contribution.

European Commission in the Collaborative Economy Communication defined the core elements of the ‘collaborative economy’ business model:

[collaborative economy] refers to business models where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals. The collaborative economy involves three categories of actors: (i) service providers who share assets, resources, time, and/or skills — these can be private individuals offering services on an occasional basis (‘peers’) or service providers acting in their professional capacity (‘professional services providers’); (ii) users of these; and (iii) intermediaries that connect—via an online platform—providers with users and that facilitate transactions between them (‘collaborative platforms’). Collaborative economy transactions generally do not involve a change of ownership and can be carried out for profit or not-for-profit.

Hence, the main elements of the definition used by the European Commission include a) intermediation of digital platforms, b) focus on accessibility rather than ownership, c) peer-to-peer services, and d) flexibility towards profit-orientation¹⁰. This broad definition might be useful for analytically distinguishing collaborative from non-collaborative platforms and business models, but it does not bear legal meaning. Therefore it is necessary to refer to the body of the EU secondary law to assess whether the provisions of the relevant directives

9 V Hatzopoulos and S Roma, ‘Caring for sharing? The Collaborative Economy under EU law’, [2017] Common Market Law Review.

10 European Parliament, ‘A European agenda for the collaborative economy’ (Briefing) PE 593.510.

and regulations formulate legal criteria for the classification of a platform as a ‘collaborative economy platform’.

Within the scope of this contribution, two more established acts of the law of the EU are scrutinized. eCommerce Directive - Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) – is the first in chronological order.¹¹ The legal act entered into force before the business models based on the concept of the collaborative economy were widely established in the Internal Market, however, the Court of Justice of the European Union used this legal act as a point of reference for the judgements in cases related to the activities of the two most established companies – Airbnb and Uber. In the judgement of 20 December 2017 in the case, C–434/15 *Asociación Profesional Elite Taxi*¹² the Court referred to the art 2(a) and the definition of the ‘information society services’ (with the negative outcome for the business activity of Uber constituting ‘services in the field of transport’)¹³. The same provision was revoked in the judgement of 19 December 2019 in case C–390/18 *Airbnb Ireland*,¹⁴ however with a different outcome¹⁵ – the activity of Airbnb was found to meet the cumulative criteria for ‘information society services’¹⁶. Therefore the definition of ‘information society services’ could not provide a consistent framework for various models pursued by collaborative economy platforms (in the sense of the non-legal definition of the European Commission cited above). Hence the definition of the ‘information society services’ might or might not, depending on the range of circumstances (economic sector, extent of control between the platform and the conditions offered by users, existence of sectoral legislation), rather than the core business model, cover the activities of the platform¹⁷. Hence, it does not increase the level of legal certainty of the platform users and does not bring definitional clarity to

11 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) [2000] OJ L 178/1, hereinafter eCommerce Directive.

12 Case C–434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain SL* [2017] ECLI:EU:C:2017:981.

13 M Finck, ‘Distinguishing internet platforms from transport services: *Elite Taxi v. Uber Spain*’, [2017] Common Market Law Review.

14 Case C–390/18 *Criminal proceedings against X with the intervention of Airbnb Ireland UC and others* [2019] (hereinafter *Airbnb Ireland*).

15 C Busch, ‘The Sharing Economy at the CJEU: Does Airbnb pass the “Uber test”?’ [2018] Journal of European Consumer and Market Law.

16 P Van Cleynenbreugel, ‘Accommodating the freedom of online platforms to provide services through the incidental direct effect back door: *Airbnb Ireland*’, [2020] Common Market Law Review.

17 A De Franceschi, ‘Uber Spain and the “Identity Crisis” of Online Platforms’, [2018] Journal of European Consumer and Market Law, 1.

the question of whether the eCommerce Directive could provide a meaningful legal framework for the activities of the ‘collaborative economy platforms’ in the Internal Market¹⁸.

Hence, it is worth analyzing the potential of the Services Directive – Directive 2006/123/EC on services in the internal market – in this respect.¹⁹ Once regarded as the horizontal and cross-sectoral legislation encompassing the freedom of movement of services in the Internal Market it was also used as a point of reference by the Court in the two fundamental cases cited above. However, in this context the consistency was also not represented by the Court – in *Elite Taxi* the Court classified the activity of Uber as ‘services in the field of transport’ within the meaning of the art 2(2)(d) of the Services Directive. In *Airbnb Ireland*, the Court assessed that the ‘activity of intermediation at issue in the main proceedings [provided by Airbnb] comes under the notion of ‘service’ within the meaning of [...] the Services Directive’. However, the definition of ‘service’ is arguably too wide and does not provide the required specification of the business models of collaborative economy platforms. At the same time, this definition is not always met in case of the activities pursued not for profit (between the users) and for the activities of the platforms themselves the more specific definition of ‘information society services’ will be simultaneously met (as in the case *Airbnb Ireland*). Hence the Services Directive also does not provide definitional clarity, nor increases level of the legal certainty regarding the activities of collaborative economy platforms in the Internal Market.

In this context, two major legal acts adopted in recent years in the domain of the EU digital law – Digital Services Act (DSA)²⁰ and Digital Markets Act (DMA)²¹ adopted and entered into force in 2022 – could provide remedies to the definitional deficiencies of the EU law towards collaborative economy platforms presented above. However, neither DSA nor DMA contains an explicit definition of a ‘collaborative economy platform’. Nevertheless, in the art 1(1) of the DSA the aim of the regulation is stipulated in the following manner:

The aim of this Regulation is to contribute to the proper functioning of the

18 C Wendehorst, ‘Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive’, [2016] Journal of European Consumer and Market Law, 1.

19 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [2006] OJ L 376/36 (Services Directive) [2006] OJ L 376/36.

20 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, hereinafter DSA.

21 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265, hereinafter DMA.

internal market for intermediary services by setting out harmonised rules for a safe, predictable, and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.

The term ‘intermediary services’ is not however defined in the art 3 named ‘Definitions’, therefore according to recital n 1 it should be interpreted as one of the ‘information society services’ used in the eCommerce Directive.

DMA in the art 2(5) defines ‘online intermediation services’ through reference to the so-called ‘P2B Regulation’²². The P2B Regulation defines 3 cumulative criteria for the definition of ‘online intermediation services’ – 1) they have to constitute ‘information society services’ in the meaning of the eCommerce Directive, 2) they facilitate the offering of goods and services by businesses to the end consumers irrespective of where those transactions are ultimately concluded, 3) the services are provided based on contractual relationships between business users and providers of services. Intriguingly recital n 11 of the P2B Regulation indicates examples of the ‘online intermediation services’ that could ‘include online e-commerce market places, including collaborative ones on which business users are active, online software applications services, such as application stores, and online social media services, irrespective of the technology used to provide such services’.

Thus it seems that the collaborative economy platforms could be covered by both P2B Regulation and DMA as the platform providing ‘online intermediation services’²³. A similar conclusion could be drawn to the ‘intermediary services’ covered by DSA. However, none of these legal acts (neither DSA nor DMA) differentiates between the collaborative economy platform and other online platforms. Hence, no specific definition for the collaborative economy platforms in the analysed EU legislation could be determined. It has its impacts on the possibility to determine applicable legal framework to their activities and requirements that are imposed on them by the provisions of the EU law. These matters are presented in the following section of this paper.

3. Failed attempts to find a suitable legal framework in the EU law – eCommerce Directive and Services Directive

Firstly, it needs to be assessed to what extent the eCommerce Directive and Services Directive has established suitable legal frameworks for the operations

²² Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57.

²³ C T Flesner, ‘The EU’s Proposals for Regulating B2B Relationships on online platforms – Transparency, Fairness and Beyond’, [2018] Journal of European Consumer and Market Law.

of the collaborative economy platforms in the EU. In this context, these legal acts have shown some shortcomings in capturing the specificities of the collaborative economy platforms. The issue of the applicability of the EU legal regime deserved some attention from scholars in the context of the scope of application of the Services Directive. The possibility to use its framework for specific and new emerging business models was discussed before, however, the conclusions from these analyses are inconsistent²⁴. This is also reflected in the fragmentation of national approaches towards various business models associated with collaborative economy platforms²⁵. As the practice shows, correct classification of the activity and applicable EU law is of fundamental importance for the conformity of new legal regimes introduced by the Member States for collaborative business models with EU law.

Two possibilities to classify the activity of most practice-relevant platforms were presented in the literature and were also present in the Court examination in cases related to the activity of collaborative economy platforms in the Internal Market. The first approach was based on the premise that collaborative economy platforms provide only the services of digital intermediation between the provider and recipient of the final service. The second approach assumes that the collaborative economy platforms provide final services through the offering of digital means and take responsibility for the provider of the downstream service to the end user. In this context, it is worth noting that the Court had to balance the free flow of services in this very particular field (with all the reasoning related to the innovativeness of the digital economy and benefits for the consumers) with other reasons of public interest²⁶. As the analysis shows, the Court paid also due attention to maintaining flexibility and equilibrium between the need to establish a coherent framework for providers of services (enabling roll-out and scale-up of collaborative economy platforms on the Internal Market) with the Member States competence to define the desired level of regulation in the fields of shared competencies.

The Court scrutinized business models of collaborative economy platforms in two sectors: transport and accommodation. The fundamental ruling for the first group was issued in 2017 in the case *Asociación Profesional Élite Taxi*. In this judgement, the Court remarkably declared services provided by the Uber

24 See *inter alia* M Inglese, 'The Collaborative Economy Legal Conundrum: A Way Forward Through Harmonization', [2018] Legal Issues of Economic Integration; M J Sorensen, 'Private Law Perspectives on Platform Services. Uber – a business model in search of a new contractual legal frame?', [2016] Journal of European Consumer and Market Law.

25 Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, M Naumanen, and others, *Study to monitor the business and regulatory environment affecting the collaborative economy in the EU : final report* (Publications Office of the European Union 2018).

26 S Ganapati, C G Reddick, *Prospects and challenges of sharing economy for the public sector*, (2018) 35 Government Information Quarterly.

company as having the nature of services in the field of transport and not ‘information society service’²⁷. The Court laid out the precise conditions under which it is possible to determine whether a collaborative economy platform ‘exercises decisive influence over the conditions under which the service is provided’ – i.a. setting prices, and automated choice of the available drivers and routes²⁸. The result of this examination led the Court to the conclusion that such a situation is confirmed in the case of the services provided by Uber users and thus the activity of Uber is inherently linked to these services. Hence, the collaborative economy platform provides services in the field of transport which are excluded from the scope of application of the Services Directive²⁹. These remarks were repeated and further confirmed by the Court in the *Uber France* case³⁰. This approach was also applied by the Court in the more recent case *Star Taxi App* where the Court assessed whether the activity of the platform provider includes exerting a decisive influence on the conditions of the service. The result of this analysis was negative in this case (as suggested by the national court presenting the preliminary question) because the platform limited its activity to pure intermediary services, without directly interfering with the conditions of the downstream service (pricing, choosing providers, or processing payments)³¹. Thus, the applicable regime had to be decided between the regime of the Services Directive and the eCommerce Directive.

This analysis, also presented by the Court in the case *Airbnb Ireland*, enabled insight into the Court’s argumentation on delimitation between the legal regimes of the Services Directive and the eCommerce Directive. In both cases, *Airbnb Ireland* and *Star Taxi App* the Court indicated the general derogation of the art 3 of the Services Directive as a general collision clause³². Further, the Court declared the intermediary activity between hosts and accommodation seekers as constituting an ‘information society service’ because the platform of Airbnb did not exercise ‘decisive influence over the conditions under which the service is provided’ and provided services ‘distinct from the subsequent service to which it relates’³³ – hence in the case of services offered by Uber the user is provided with one unitary service of transport and in the case of services offered by Airbnb these are two separate services – intermediation in finding short-term accommodation provided by Airbnb and final service of

27 Schaub M.Y., ‘Why Uber is an information society service’, [2018] Journal of European Consumer and Market Law, 109.

28 See *Asociación Profesional Elite Taxi* (n 12), para 39.

29 *ibid* paras 40–43.

30 Case C–320/16 *Uber France SAS* [2018] ECLI:EU:C:2018:221 paras 22–25.

31 Case C–62/19 *Star Taxi App SRL v Unitatea Administrativ Teritorială Municipiul București prin Primar General and Consiliul General al Municipiului București* [2020] ECLI:EU:C:2020:980, paras 39–40 and paras 51–55.

32 *Airbnb Ireland* (n 14) para 41 and *Star Taxi App* (n 31) para 78.

33 *Airbnb Ireland* (n 14) paras 42–68.

accommodation provided by another user of the platform. The Court confirmed that services of renting accommodation were clearly within the scope of the application of the Services Directive, but since the conditions laid out in the directive on ‘information society services’ have been cumulatively fulfilled, the activity of Airbnb has been expelled from the scope of the Services Directive and analyzed in the light of (more liberal) provisions of the eCommerce Directive.

The analysis of the Court presented in the *Airbnb Ireland* ruling was very detailed and delivered mainly in the context of the arguments of the parties on the similarities of services of Airbnb and Uber and therefore focused on the conditions from the *Asociación Profesional Élite Taxi* and ‘the exercise of decisive influence’ to determine whether the ‘intermediation service [can] be separated from the property transaction itself’ and forms ‘an integral part of an overall service whose main component is a service coming under another legal classification’³⁴. These remarks were invoked in the *Star Taxi App* and referred to as ‘established case law’³⁵ – as such it might be regarded as the general approach to identifying a suitable legal framework for the services of the collaborative economy platforms. The character of the ‘information society service’ has been also attributed to the activity of the *Star Taxi App*³⁶, however, the Court did not automatically exclude it from the scope of the Services Directive. It concluded that for the exclusion provided by art 3(1), it has to be determined whether the collision between the Services Directive and other legal acts regulating providing of services in different economic sectors truly occurs³⁷. In this context the Court observed that it is the case only when the restrictions (preliminary authorization) imposed by the Member States are aimed specifically at the ‘information society services’ and if they have more general character (ie refer to all methods of intermediating between providers and consumers including radio), they should be interpreted solely in the context of conformity with the provisions of the Services Directive³⁸.

This approach towards platforms itself was contrasted with the ruling of the Court in *Cali Apartments*, where not the activities of the platforms but of the providers using them to offer their services (accommodation) were scrutinized. The Court in the straightforward interpretation of the definition of ‘service’ provided by the art 4(1) of the Services Directive applied its provisions to the

34 See *Airbnb Ireland* (n 32) paras 50–68.

35 See *Star Taxi App* (n 31) para 49.

36 See *Star Taxi App* (n 31) paras 41–48.

37 See *Star Taxi App* (n 31) para 79.

38 See *Star Taxi App* (n 31) paras 80–84; see also W Lewandowski, ‘Removing Barriers to Trade in Services in the Single Market with the Help of the Services Directive – Assessment of the Recent Case Law of the Court of Justice’ (2022) 18/1 *Utrecht Law Review*, 57–75 <<https://doi.org/10.36633/ulr.718>> accessed 30 May 2024.

‘repeated short-term letting, for remuneration, whether on a professional or non-professional basis, of furnished accommodation to a transient clientele which does not take up [permanent] residence’³⁹. The Court found that the restrictions provided for such activity by national legislation fall within the scope of the Services Directive when they are intended to regulate access to, and the exercise of, these services provided by private individuals⁴⁰ which might impact the activities of the collaborative economy platforms. Many of such restrictions adopted by the national and local authorities resulted from the rise in popularity of the business models of the collaborative economy platforms and enabled new avenues for offering the services to their users⁴¹. The Court denied by this occasion arguments brought by intervening Member States on the ‘hidden’ purpose of the legislation limiting such possibility to specified periods potentially excluding it from the scope of application of the Services Directive⁴². The Court reiterated that even if the national legislation is aimed at regulating some activities falling outside the scope of application of the Services Directive, this ‘mere fact’ is not enough to exclude this legislation altogether from the scope of application of the Services Directive when it covers also services not explicitly excluded from the Services Directive. Therefore the prevailing character has to be given to the effectiveness of the Services Directive without calling into question the objective thereof - ‘establishing an area without internal frontiers in which the free movement of a wide variety of services is ensured’⁴³.

However, the Court showed some degree of awareness of the impacts that the preference for the Services Directive over the national legislation might result in. While applying the provisions of the Services Directive the Court tried to carefully assess all the circumstances to determine the applicable legal regime, allow for reaching the main objectives of the Services Directive but also balance it against other legitimate interests pursued by the legislation of Member States. The application of the Services Directive to the activity of collaborative economy platforms (and its users) serves as the best example of how unintuitive this task is when these contrasting interests are on display. The Court formulated specific guidelines for the analysis of whether the activity of the platform falls within the scope of the Services Directive or gets excluded

39 Case C-724/18 *Cali Apartments SCI and HX v Procureur général près la cour d’appel de Paris and Ville de Paris* [2020] paras 31–36.

40 See *Cali Apartments* (n 39) paras 44–45.

41 V Mak, ‘Private Law Perspectives on Platform Services. Airbnb: Home Rentals between AYOR and NIMBY’, [2016] *Journal of European Consumer and Market Law*.

42 See *Cali Apartments* paras 37–42. Intervening Member States indicated at the ‘hidden’ purposes in form of ‘the change of use of residential premises (...) for the purpose of accommodating homeless persons or refugees’ (non-economic service of general interest covered by the art 2(2)), ‘rules concerning the development or use of land [and] town and country planning’ (exclusion of spatial planning covered by the recital n 9).

43 See *Cali Apartments* (n 39) para 39.

– which are followed by the national courts with good measure⁴⁴. Hence, it can be observed that the Court tried to apply the existent EU law provisions to the innovative business models of the collaborative economy platforms. It did so by presenting clear criteria whether the platform ‘exercise decisive influence on the conditions of the service’, whether providing ‘intermediation service [can] be separated from the [service] itself’, and whether the activity of collaborative economy platform forms ‘an integral part of an overall service’ which are crucial to determine whether the platform provides entire (upstream and downstream) service to the consumer (which could be excluded or not excluded from the scope of the Services Directive depending on the economic sector). Or whether the platform provides an intermediary ‘information society service’ covered by the regime of the eCommerce Directive. The Court went also into detail to analyze whether the real collision between the regimes of the Services Directive and the eCommerce Directive occurs to preserve preferential treatment of digital platforms to other, more conventional, forms of intermediating and thus avoided the ‘digital first’ approach. It follows, from the analysis that the Court was capable of flexibly adapting the argumentation and choosing applicable legal regimes to ensure the maximum level of liberalisation without undermining the minimum level of protection of other competing reasons of general interest. The Court had to be creative to some degree to fill the legislation void and *legal vacuum* and lack of a dedicated legal regime in the EU law which could provide a regulatory response to the dilemmas above. Therefore it is worth presenting whether the adoption of the landmark legislation for the EU digital policy – DSA and DMA – provided remedies to the situation cured previously by the Court with the creative criteria for applying Services Directive and eCommerce Directive.

4. DSA & DMA and regulating the activities of the collaborative economy platforms

In Section 2 it was determined that neither DMA nor DSA define collaborative economy platforms. Hence, they don’t directly refer to the business models of collaborative economy platforms. However, DSA includes reference to ‘intermediary services’, and DMA to ‘intermediation services’, therefore these kinds of activities remain within the scope of either of this legislation. Knowing that the application of the right regime of the EU law to the collaborative economy platform depends on the degree of strictness (‘exercising decisive influence’) in ‘intermediating’ between service providers and recipients it could be possible to determine whether DSA and DMA could establish a suitable legal

44 As the analysis of Romanian court in the *Star Taxi App* on the character of the service provided by the platform in the main proceedings got endorsed by the Court.

framework for ‘intermediary services’ and ‘intermediation services’ provided by the collaborative economy platforms.

Art 1 of DSA determines in this context the aim of the regulation to ‘contribute to the proper functioning of the internal market for intermediary services’ through the adoption of harmonised rules for safety, predictability, and trust in the online environment, facilitation of innovation and effective protection of the EU fundamental rights enshrined in the Charter. Specifically, the harmonisation of DSA should consist of the establishment of a) framework for the liability of providers of intermediary services, b) specific due diligence obligations for specific categories of providers, and c) implementation and enforcement rules. *Prima facie* these obligations and frameworks do not address the specificity of business models of the collaborative economy platforms. The obligations provided by DSA refer to the transmission of information (‘mere conduit’), storage (‘caching’ and ‘hosting’), monitoring, combating illegal content, and reporting on moderating of the information. Certain specific obligations for ‘providers of online platforms allowing consumers to conclude distance contracts with traders’ and ‘providers of very large online platforms and of very large online search engines’ are also determined, however, they do not tackle activities of collaborative economy platforms defined in the Commission communication (intermediation between peer-to-peer service providers and recipients). It is also evidenced by the lack of collaborative economy platforms in the list of very large online platforms and very large online search engines published in April 2023 by the European Commission⁴⁵. This is not to say that the collaborative economy platforms are excluded from the scope of application of DSA, however, their business model is not the subject of obligations and/or reporting requirements – for example, they might be faced with the consequences for not addressing abusive or discriminatory content in the information transmitted by the users through the platform⁴⁶. Nevertheless, the users of the collaborative economy platforms will not be able to determine the provisions directly addressing the substance of the business models pursued by them.

The objective of DMA is in turn described as a contribution to the proper functioning of the internal market by ensuring ‘for all businesses’ contestability and fairness in the markets in the digital sector across the Union, especially in the markets with the presence of gatekeepers – ‘to the benefit of business users and end users’. The scope of application is determined on the premise of ‘core platform services provided or offered by gatekeepers’ to businesses and

45 Commission, ‘Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines’ (European Commission 2023), <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413> accessed 30 May 2024.

46 S Navas Navarro, ‘Discrimination and Online Platforms in the Collaborative Economy’, [2019] Journal of European Consumer and Market Law.

consumers located in the EU. To this end, ‘online intermediation services’ were defined as one of the core platform services, and through the reference to the definition of ‘online intermediation services’ included in the P2B Regulation, it could extend to the collaborative economy business models. Consequently, the activity of collaborative economy platforms might be directly covered by DMA provisions if they are designated as gatekeepers (ie meet the criteria set out in the art 3 of DMA – turnover, number of users, and permanent presence in the Internal Market⁴⁷). This designation is not without practical problems, but given the high threshold set in the final wording of the DMA, it can be expected that only the biggest platforms, such as Uber or Airbnb could be considered as gatekeepers⁴⁸. However, bearing in mind that Uber was previously classified as a provider of services in the field of transport due to its ‘decisive influence’ on the conditions of the service provided, it might further limit the list. What kind of obligations might then be imposed on the collaborative economy platforms by DMA?

DMA stipulates obligations for data access and usage, distribution, bundling, and interoperability of digital services, non-discriminatory treatment and preventing self-preferencing, granting access to search engine data and effective access to key core platform services, enabling interoperability of messaging services, as well as compliance and reporting obligations. DMA to a large extent codifies existing case law of the Court and the Commission in the field of competition law application toward digital companies⁴⁹ and it is evident that the main objective is to ensure wide access to markets created or maintained by the platform operators and fair competing conditions thereon⁵⁰ – this is very relevant objective to the activity of collaborative economy platforms who intermediate between service providers and recipients and thus create markets for the exchange of these services. Therefore DMA could become a relevant framework for the activities of the biggest collaborative economy platforms⁵¹, but the conditions set out for gatekeepers leave the majority of these entities outside of its scope.

47 M Eifert and others, ‘Taming the Giants: The DMA/DSA package’, [2021] Common Market Law Review, 987–1028.

48 M Mariniello, C Martins, ‘Which platforms will be caught by the Digital Markets Act? The “gatekeeper” dilemma’ (*Bruegel* 14 December 2021) <<https://www.bruegel.org/blog-post/which-platforms-will-be-caught-digital-markets-act-gatekeeper-dilemma>> accessed 30 April 2023.

49 N Nicoli, P Iosifidis, ‘EU digital economy competition policy: From ex-post to ex-ante. The case of Alphabet, Amazon, Apple, and Meta’ (2023) 8 *Global Media and China*, 24–38.

50 Recitals 1–7 DMA.

51 M Cian, ‘Online Platforms as Gatekeepers to the Digital World – A Preliminary Issue on Business Freedom, Competition and the Need for a Special Market Regulation’, [2018] *Journal of European Consumer and Market Law*.

Therefore, to assess whether DSA and DMA would constitute a suitable legal framework for the activity of collaborative economy platforms it is necessary to refer to the wider objectives of the digital policy of the EU towards collaborative economy platforms. In this context, it is worth interpreting the obligations on collaborative economy platforms by DSA and DMA in light of the objectives laid out in the Collaborative Economy Communication of the Commission from 2016. The Commission back then determined several issues that should be resolved to reach two main policy objectives – supporting consumers, businesses, and public authorities to engage confidently in the collaborative economy and enabling consistent application of the EU law across the Internal Market. These issues were most notably market access, liability regimes, protection of users, taxation, and status of self-employed and workers in the collaborative economy.

Against this background, it should be noted that the framework provided by DMA and DSA is partially relevant. DSA and DMA are both regulations, hence are effective directly and impose uniform EU-wide standards. Thereby they create common requirements for market access for (foreign) collaborative economy platforms. However, uncertainty remains whether this approach will not be differentiated by criteria of the economic sector (different regime of the services in the field of transport vs. intermediating in finding short-term accommodation), possibility to adopt national regulations under different EU legislation regimes (Services Directive, DSA, DMA, eCommerce Directive) and/or fragmentation of the framework for activities of the largest ‘gatekeepers’ (Uber, Airbnb) and platforms of smaller size (Bolt, Slowhop or other regional providers). It will have also an impact on the liability regimes that could be adopted at the EU level or national depending on various circumstances, including the ‘exercise of influence over the conditions of the services’ that the platforms adopt for their business models. However, this is the area in which DSA could provide the most significant response to the issues described by the Commission in the Collaborative Economy Communication. DSA constitutes also a positive development in the sphere of the protection of users (as well as P2B Regulation that remains outside of the scope of this contribution), however not necessarily in the context that was meant in the Collaborative Economy Communication (consumer law protection, marketing rules, online rating, and review systems, quality of services, transparency requirements and data protection)⁵². The status of workers and self-employed⁵³, as well as taxation, remain outside the scope of DSA and DMA and thus will not be elaborated further in this contribution.

52 C Busch and others, ‘The Rise of the Platform Economy: A New Challenge for EU Consumer Law?’, [2016] *Journal of European Consumer and Market Law*.

53 S Nerinckx, ‘The “Uberization” of the labour market: some thoughts from an employment law perspective on the collaborative economy’, (2016) 17 *ERA Forum*.

For all the above presented reasons it seems that the policy objectives of ensuring confidence and increased legal certainty, as well as avoidance of fragmentation, were not fully met with the adoption of DSA and DMA. Several important questions related to the applicable legal regime and relevant EU legal framework for the operations of collaborative economy platforms remain unresolved. Among them, the most important is the question about responsibility for the quality of the service provided. It remains a *case-by-case* issue that is differently approached among various national legal orders (for example the obligation for the licensing of Uber drivers) and hence leads to the fragmentation of the Internal Market and level of protection of users in different Member States. At the same time, the application of the obligations from DMA, the initiative that might be of the biggest practical relevance, will be limited to two-three major collaborative economy platforms, but will not result in the trickling-down of regulatory standards and the emergence of spill-over effects is not a given. Hence, the potential of DSA and DMA to fill the legal *vacuum* identified before concerning the suitable framework for activities of the collaborative economy platforms in the Internal Market will not be fulfilled entirely⁵⁴. The question remains with what impacts it could result on the users of these platforms and the implementation of the digital policy of the EU.

5. Transnational collaborative economy platforms and the EU digital policy

The collaborative economy constitutes an interesting example of an unfulfilled promise. Back in 2016, it was described by the Commission in the language of hope and anticipation of wider use of business models pursued by platforms in the EU:

The collaborative economy creates new opportunities for consumers and entrepreneurs. The Commission considers that it can therefore make an important contribution to jobs and growth in the European Union if encouraged and developed in a responsible manner. Driven by innovation, new business models have a significant potential to contribute to competitiveness and growth. The success of collaborative platforms are at times challenging for existing market operators and practices, but by enabling individual citizens to offer services, they also promote new employment opportunities, flexible working arrangements and new sources of income. For consumers, the collaborative economy can provide benefits through new services, an extended supply, and lower prices. It can also encourage more asset-sharing and more efficient use of resources, which can contribute to

54 J Laux, S Wachter, B Mittelstadt, 'Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA', (2021) 43 Computer Law & Security Review 105613.

the EU's sustainability agenda and to the transition to the circular economy.

However, after 7 years it could be difficult to argue that this hope materialised. In the literature it was observed that the collaborative economy '*leads to a paradox; since for some researchers it is regarded as a response to the capitalist economy, viewed as an alternative to that, and on the other hand, other researchers regard it as part of the same system*'⁵⁵. This context of the role that collaborative economy and collaborative economy platforms could exercise in the Internal Market has been present to a limited extent in Collaborative Economy Communication⁵⁶. However, the disruptive potential of innovation brought by the business models based on sharing and using rather than owning has been indeed regarded as one of the most promising aspects of the activity of collaborative economy platforms⁵⁷. Unfortunately, the uncontrolled rise in popularity, dumping of quality and safety of services, negative impacts on the environment, and the need to protect justified public interest against the risk of exploitation increased the regulatory activity at the Member States and local level⁵⁸. Therefore platforms have been very active and using various lobbying and 'stalling' strategies to prevent or influence the adoption of such regulations⁵⁹.

To a large extent successfully – as the recent scandal showed, the collaborative economy platforms have been very efficient in lobbying among top policymakers and could favorably influence decision-making processes⁶⁰. This might partially explain the lack of consistency in regulating the activity of collaborative economy platforms at the national level among Member States. To better understand this effect it might be also useful to refer to the concept of 'transnational organisations' – organisations that are of private origin, have an international scope of activities and economic power allowing them to engage at the political level on equal (or even sometimes prevailing) terms with the

55 T Daglis, 'Sharing economy', (2022) 2 Encyclopedia 1322–1332 <<https://doi.org/10.3390/encyclopedia2030088>> accessed 30 May 2024.

56 C Cauffman, *The Commission's European Agenda for the Collaborative Economy – (Too) Platform and Service Provider Friendly?*, [2016] *Journal of European Consumer and Market Law*.

57 K Gruszka, 'Framing the collaborative economy – Voices of contestation', (2017) 23 *Environmental Innovation and Societal Transitions*. See also: C J Martin, P Upham and R Klapper, 'Democratising platform governance in the sharing economy: An analytical framework and initial empirical insights', (2017) *Journal of Cleaner Production*, 165.

58 J Kociubiński, 'Regulating Sharing Economy – Interplay Between Private Law and Public Law', [2018] *Gdańskie Studia Prawnicze*.

59 J Mazur, M Serafin, 'Stalling the State: How Digital Platforms Contribute to and Profit From Delays in the Enforcement and Adoption of Regulations' (2023) 56/1 *Comparative Political Studies* 101–130.

60 The uber files: Rob Davies, 'How the leak prompted outrage across the world' *The Guardian*, (London, 15 July 2022) <<https://www.theguardian.com/news/2022/jul/15/the-uber-files-how-the-leak-prompted-outrage-across-the-world>> accessed 30 April 2023.

national states⁶¹. The EU in this context is envisaged as a public organisation of sufficient size and market power to provide effective remedies to the imbalance of powers between private and public and ensure a legal framework for the operations of such ‘transnational’ companies in the Internal Market⁶². The EU might in this respect use the leverage of market access to impose certain obligations and requirements and thus grant a higher level of protection for the rights of individuals than national states – this process leads also to closer integration within the EU itself⁶³. The EU is also well positioned to increase accountability and transparency of operations of transnational private entities by imposing commitments to the EU standards, mandatory requirements, and legislation. It is a matter of policy and political choices regarding how vigilant the EU will be in exercising these capabilities and what would be the resulting political economy outcome.

This counter-balancing power of the EU, combined with its market and regulatory power called the ‘Brussels Effect’⁶⁴, is, in particular, relevant for the digital policy⁶⁵, in which the EU has established international standards for the protection of private data, Artificial Intelligence and recently intervened with the adoption of DSA and DMA to increase accountability of the operators of large online platforms⁶⁶. Therefore the lack of an analogous proactive regulatory approach of the EU in the context of the collaborative economy platforms is meaningful and translates into a reduced level of protection of individuals concerning the collaborative economy platforms. It is simultaneously observed, that the EU adopted a more interventionist model towards digital policy in recent years⁶⁷ which has also repercussions for the geopolitical ambitions of

61 J W Cioffi, M F Kenney, J Zysman, ‘Platform Power and Regulatory Politics: Polanyi for the twenty-first century’, (2022) 27/5 *New Political Economy* 820–836.

62 A Menon, S Weatherill, ‘Transnational legitimacy in a globalising world: How the European Union rescues its states’, (2008) 31/3 *West European Politics* 397–416.

63 A Bendiek, ‘The Impact of the Digital Service Act (DSA) and Digital Markets Act (DMA) on European Integration Policy’, (2021) *Stiftung Wissenschaft und Politik Working Paper Research Division EU/Europe* 2021, 2, <https://www.swp-berlin.org/en/publication/the-impact-of-the-digital-service-act-dsa-and-digital-markets-act-dma-on-european-integration-po> accessed 7 May 2023.

64 A Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2021).

65 A Bendiek, I Stuerzer, ‘The Brussels effect, European regulatory power and political capital: Evidence for mutually reinforcing internal and external dimensions of the Brussels effect from the European digital policy debate - digital society’, [2023] *Digital Society* <<https://doi.org/10.1007/s44206-022-00031-1>> accessed 30 April 2023.

66 P Alexiadis and A De Streel, ‘Designing an EU intervention standard for digital platforms’, (2020) *European University Institute Working Paper EUI RSCAS*, 2020/14 <<https://cadmus.eui.eu/handle/1814/66307;jsessionid=8FBF4C41079B8927A88B9EEEC600F33C>> accessed 30: May 2024.

67 S Heidebrecht, ‘From market liberalism to public intervention: Digital Sovereignty and changing European Union Digital Single Market Governance’ [2023] *Journal of Common Market Studies* (JCMS).

the EU and the context of EU-US strategic partnership and ‘coopetition’⁶⁸. Therefore, the observed, fragmented, approach towards regulating the collaborative economy platforms is rather an exception than the rule in the context of the digital policy of the EU⁶⁹.

This exception causes several issues of policy and political economy nature. Firstly, as observed above, the lack of a suitable legal framework for the collaborative economy platforms at the EU level leads to the fragmentation of the level of protection and effective transfer of the regulation competencies at the national level. It follows mostly from the judgements of the Court in the cases of *Association Elite Taxi* and *Airbnb Ireland*. In the case of Uber activity and the ‘services in the field of transport,’ Member States maintain competencies to regulate access to the market, licensing, and other issues related to the business models of personal transport providers. In the case of accommodation services and the business model of Airbnb, the intermediation services of the platform have been classified as ‘information society service’ and thus subject to EU harmonisation by the eCommerce Directive. However, in *Cali Apartments* the Court indicated that the Member States can introduce certain limitations and obligations concerning the downstream services (accommodating), albeit in conformity with the Services Directive. Hence, the Member States (and local authorities) could introduce regulations⁷⁰ affecting the business conditions for the collaborative economy platform (availability of assets, rotation of providers of services, authorisation requirements)⁷¹. Other collaborative economy platforms remained under the radar of the EU law. Arguably because of the more national or local scale of functioning of these platforms⁷².

68 D Broeders, F Cristiano, M Kaminska, ‘In search of digital sovereignty and strategic autonomy: Normative Power Europe to the test of its geopolitical ambitions’, (2023) 61 Journal of Common Market Studies (JCMS).

69 J W Cioffi, *Beyond competition: The regulatory turn & the emerging era of intervention in platform firms & markets*, (Jacques Delors Centre, 2021) <<https://www.delorscentre.eu/en/publications/detail/publication/beyond-competition-the-regulatory-turn-the-emerging-era-of-intervention-in-platform-firms-markets>> accessed 7 May 2023.

70 K Nemeth, M Scharmer, ‘Regulating Airbnb in Austria’, [2018] Journal of European Consumer and Market Law; C Busch, ‘Regulating Airbnb in Germany – status quo and future trends’, *ibid*; J M Carvalho and P Policarpo, ‘Regulating Airbnb in Portugal’, *ibid*; R Koolhoven, ‘Regulating Airbnb in the Netherlands’, *ibid*.; A I Martínez Nadal, *Regulating Airbnb in Spain*, *ibid*. See also: I Kull I. ‘The Adequacy of Existing Estonian Laws for the Platform Economy’, [2016] Journal of European Consumer and Market Law; A De Franceschi, ‘*The Adequacy of Italian Law for the Platform Economy*’, *ibid*; J Pisuliński, ‘Internet platforms under Polish law’, *ibid*; E Terryn, ‘The sharing economy in Belgium – a case for regulation?’, *ibid*.

71 D Kramer and M Schaub, ‘EU Law and the Public Regulation of the Platform Economy: The Case of the Short-Term Rental Market’, (2022) 59 Common Market Law Review.

72 A Light and C Miskelly, ‘Platforms, Scales and networks: Meshing a local sustainable sharing economy’, (2019) 28 Computer Supported Cooperative Work (CSCW), 591–626 <<https://doi.org/10.1007/s10606-019-09352-1>> accessed 30 May 2024.

This scaling-up potential of local, EU-based providers, is in particular interesting from the perspective of the EU policy. As laid out in the Collaborative Economy Communication, the economic benefits related to the development of these innovative business models should contribute to the competitiveness and growth of the EU. Hence, the fragmentation of the EU legislative frameworks might have dual implications for the potential of increasing the competitiveness of EU companies in the digital economy (and of double adversity). Firstly, it allows the market leaders of transnational scale and US origin – most notably Airbnb and Uber – to negotiate favorable conditions for their operations in the Member States of the EU and reap the benefits of the presence in the national markets and exploit any regulatory grey zones and lack of pre-existing framework for their disruptive innovations. On the other hand, local emerging platforms from the EU have more difficulties to scale-up their activities due to 27 different regulatory regimes that apply to their operations and making it more difficult to build a presence in the whole Internal Market and develop a strong consumer base allowing to compete with the US- and China-based providers of digital solutions. Different levels of protection of consumers, diverging quality standards, and different approaches to the employment status of collaborative services providers add to the negative consequences of maintaining uniform EU standards. Legal certainty is also negatively affected in these circumstances⁷³. Hence, the rationale for legislation intervention at the EU level pertains⁷⁴, to the effectiveness of the Internal Market for the services provided by the collaborative economy platforms is currently not ensured. This is therefore surprising to observe that the EU missed the opportunity while adopting DSA and DMA to improve this situation and remained reluctant to impose more tangible and tailored obligations towards collaborative economy platforms that would enable the EU to fulfill its policy objectives. General obligations resulting from DSA and DMA for the collaborative economy platforms might be not enough to make a substantial difference in respect of the achievement of these objectives and implementing suitable legal framework, fitted for uniform regulation of their activities in the Internal Market. Therefore, the regulation model of the EU towards collaborative economy platforms might be described as ‘non-interventionist’. And thus even might strengthen the deterioration of the distribution of economic power between the users and the biggest platforms that is described as ‘neoliberalism on steroids’⁷⁵.

73 D Adamski, ‘Lost on the Digital Platform: Europe’s Legal Travails with the Digital Single Market’, [2018] *Common Market Law Review*.

74 Research group on the Law of Digital Services, ‘Discussion Draft of a Directive on Online Intermediary Platforms’, [2016] *Journal of European Consumer and Market Law*.

75 D Murillo, H Buckland, E Val, ‘When the sharing economy becomes neoliberalism on steroids: Unravelling the controversies,’ (2017) 125 *Technological Forecasting & Social Change*, <<http://dx.doi.org/10.1016/j.techfore.2017.05.024>> accessed 30 May 2024.

6. Conclusions

As presented in the introduction to this contribution, the Commission accurately diagnosed back in 2016 in the Collaborative Economy Communication the challenges related to the ambiguity and uncertainty related to the identification of applicable legal framework to the activities of the collaborative economy platforms. By doing so it awakened the hope to tackle these challenges with adequate policy and legal responses. However, as presented in Section 2, the challenges have been as basic, as identifying suitable legal definitions for the innovative and disruptive business models pursued in the Internal Market by collaborative economy platforms. In this context, DSA and DMA, two of the most recent legislation interventions in the sphere of digital policy did not provide sufficient clarity and direct criteria for the classification of activity of collaborative economy platforms as ‘intermediary services’ or ‘online intermediation services’. Nevertheless, as outlined in Section 3, the Court while applying EU law provisions (definitions from the Services Directive and eCommerce Directive) to the activities of the two most recognized collaborative economy platforms – Uber and Airbnb – adopted a proactive approach to mitigate the negative effects resulting from the lack of clarity in this respect. A legal framework could be established recently by including relevant obligations for collaborative economy platforms in DSA and DMA, however, they were neither singled out as the specific category for obligations, nor the essence of their business model has been the subject of new requirements or obligations resulting from these legal acts. Hence, the adverse impacts on the fragmentation of the Internal Market and insufficient level of safeguards for users interacting with transnational private organisations are provided. It might have negative consequences for the level of protection of users and differentiation between sectors, national borders, or the size of the platform. At the same time, it might impede the emergence of scaling-up opportunities for platforms developing in the EU. Hence, the rationale for legislation intervention has been reinforced and the result of the analysis conducted in this contribution indicates that the approach of the EU remains non-interventionist. The end result also shows that the original challenges and main issues mentioned in the Collaborative Economy Communication have not been effectively addressed by the EU legislation and therefore the policy objectives of the EU – strengthening the confidence of users, enabling a higher level of legal certainty and avoiding fragmentation in the Internal Market – remain unfulfilled.

Personal Data as Counter-Performance in Exchange for Contents or Services After Amendments to the Italian Consumer Code

Sofia Maria Lener

Università degli Studi della Tuscia, Italy

ORCID 0000-0003-1980-9152

DOI: 10.54103/milanoup.215.c454

Abstract

The Directive (EU) 2019/770 expressly regulated, for the first time, contracts where the trader supplies digital content or a digital service and the consumer does not pay a price but provides personal data. It was implemented in Italy with the Legislative Decree No. 173/2021, which amended the Consumer Code, by introducing the Chapter I-bis. However, although the Directive and, consequently, the Italian Consumer Code recognize the possibility – and therefore the lawfulness – for personal data to be exchanged for a service, they expressly exclude that personal data can be considered a commodity, comparable to a price, creating serious doubts as to their nature and the qualification of their provision. In addition, the Directive extends its scope of application to contracts for the exchange of digital services and personal data, thus generally extending the scope of consumer protection law to this relationship, but without making any coordination between the different rules, and this is particularly evident and problematic in relation to pre-contractual information and unfair commercial practices. The same can be said for Union law on the protection of personal data, expressly referred to in the Directive, which, however, leaves out the regulation of relevant issues, such as the conditions of lawfulness of processing, whether consent coincides with contractual consent and is compatible with data protection law, and what happens if it is withdrawn. By examining Directive (EU) 2019/770, the Italian Consumer Code, European consumer and data protection law, as well as the opinions of the European Data Protection Supervisor and the Italian Competition Authority, legal scholars and case law, the paper aims to address whether personal data can be considered as the payment for a service and under what conditions their processing can be considered lawful.

Keywords

Directive 2019/770, Italian Consumer Code, Nature of Personal Data, Coordination Problems, Consumer Protection Law, GDPR

1. The adoption in Italy of Directive (EU) 2019/770, the first European regulation on contracts having as consideration the providing of personal data

As part of the Digital Single Market Strategy for Europe,¹ following a complicated legislative process,² Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter, DCD, Digital Content Directive) was published on 22 May 2019.³ Member States should have transposed its content by 1 July 2021.⁴ In Italy, however, the law delegating authority to the Government to transpose the DCD was approved on 22 April 2021⁵ and finally implemented in November of the same year.⁶ The implementation of the DCD in Italy resulted in the introduction of Chapter I-*bis*, entitled ‘Of contracts for the supply of digital content and digital services’, into the Italian Consumer Code (hereinafter, CC, Consumer Code),⁷ consisting of arts 135-*octies* to 135-*vicies*, which took effect on 1 January 2022 and applies to supplies of digital content or digital services occurring on or after that date.⁸

Among the most relevant innovations of the DCD is certainly the first explicit recognition in a European law of contracts in which, in exchange for the supply of a digital content or service, the consumer provides personal data. This contractual model, indeed, is now used in various forms and with increasing intensity on the market: to mention the best known, contracts for the use of search engines or social networks fall within this model, where the service provided is apparently free of charge or, at least, is presented as such.⁹

1 Commission ‘Communication on a Digital Single Market Strategy for Europe’ COM (2015) 192 final.

2 Guido Alpa, ‘Aspetti della nuova disciplina delle vendite nell’Unione europea’ [2019] *Contratto e impresa* 825, 825–826.

3 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

4 DCD, art 24.

5 Italian Law No. 53/2021.

6 With Italian Legislative Decree No. 173/2021.

7 Italian Legislative Decree No. 206/2005.

8 Italian Legislative Decree No. 173/2021, art 2.

9 Guido D’Ippolito, ‘Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale’ [2020] *Diritto dell’informazione e dell’informatica* 635, 638; Alberto De Franceschi, ‘Il “pagamento” mediante dati personali’ in Vincenzo Cuffaro, Roberto D’Orazio

The personal data collected in this way are then used for various purposes, including profiling users in order to produce targeted advertisements or to offer goods and services in line with individual tastes. In particular, these data enable companies to obtain highly detailed knowledge of the needs and preferences of individual consumers that can be used to achieve a high degree of customisation of the products and services offered, which is particularly relevant for online advertising and e-commerce.¹⁰ Hence the enormous relevance of Big Data,¹¹ defined in the scientific literature through the ‘4 Vs’: the *volume* of data collected, the *variety* of sources, the *velocity* with which data analysis can take place and the *veracity* of the data that could (presumably) be achieved through the analytical process¹² or, alternatively, the *value* that the data assume when analysed.¹³ But at the same time, new risks arise in terms of competition, protection of personal data and information pluralism.

Therefore, in the light of the increasing popularity of contracts in which the counter-performance consists of personal data – and the resulting risks – one cannot but look favourably on the first attempt to regulate this contractual scheme.

More specifically, the DCD applies to two contractual models of supply,¹⁴ namely, any contract where the trader supplies a digital content or a digital service and the consumer pays a price and where the trader supplies a digital content or a digital service and the consumer provides personal data, except

and Vincenzo Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli 2019) 1382; Giorgio Resta and Vincenzo Zeno-Zencovich, ‘Volontà e consenso nella fruizione dei servizi in rete’ [2018] *Rivista trimestrale di diritto e procedura civile* 411, 414.

10 Italian Communications Regulatory Authority, Competition Authority and Data Protection Authority, ‘Indagine conoscitiva sui *Big Data*’ (2020) <<https://www.agcom.it/>> accessed 30 April 2023, 19.

11 Indeed, the Big Data market in Italy has been growing for years: the Big Data & Business Analytics Observatory of the Politecnico di Milano estimated that the Italian Data Management e Analytics market grew by 20 per cent in 2022, reaching a value of more than EUR 2 billion (‘Il tasso di crescita del mercato analytics in Italia, 2017-2022’ (2023) <<https://www.osservatori.net/it/prodotti/formato/grafici/il-tasso-crescita-mercato-analytics-italia-2017-2022-grafico>> accessed 30 April 2023) and Statista predicts that the global Big Data market will grow to USD 103 billion by 2027 (‘Big data market size revenue forecast worldwide from 2011 to 2027’ (2022) <<https://www.statista.com/statistics/254266/global-big-data-market-forecast/>> accessed 30 April 2023).

12 Svetlana Sicular, ‘Gartner’s Big Data Definition Consists of Three Parts, Not to Be Confused with Three “V”s’ (2013) *Forbes* <<https://www.forbes.com/sites/gartner-group/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/>> accessed 30 April 2023; ‘IT Glossary: Big Data’ Gartner <<https://www.gartner.com/en/information-technology/glossary/big-data>> accessed 30 April 2023.

13 Italian Communications Regulatory Authority, Competition Authority and Data Protection Authority (n 10) 8.

14 Carmelita Camardi, ‘Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali’ [2019] *Giustizia civile* 499, 505.

where the personal data provided are processed exclusively for the purpose of supplying the digital content or the digital service or for allowing the trader to comply with legal requirements to which the trader is subject.¹⁵

For the second type of contract, it is stipulated that European data protection law applies and that, notably, in the event of a conflict between DCD and data protection laws, the latter will prevail.¹⁶

As a general rule, the Directive regulates only certain aspects of contracts for the supply of digital content or digital services concluded between a consumer and a trader, including the conformity of the digital content or digital service with the contract, remedies in the event of a lack of such conformity or a failure to supply and the modalities for the exercise of those remedies, as well as on the modification of digital content or a digital service.¹⁷ It does not, therefore, affect the law of the Member States concerning matters not expressly regulated: in Italy, pursuant to art 135-*viciester* CC, the contracts in question are subject to the provisions of the Italian Civil Code on the formation, validity and effectiveness of contracts, including the consequences of the termination of the contract and the right to compensation for damages.

In order to conform with the contract, the digital content or digital service must meet certain subjective¹⁸ and objective¹⁹ requirements, and the trader is obliged to keep the consumer informed of available updates necessary to maintain the conformity of the digital content or digital service.²⁰

The trader is liable for failure to supply the content or service, as well as for any lack of conformity that becomes apparent within two years from the time of supply.²¹ In both cases, the burden of proof is, as a rule, on the trader.²² In the event of failure to supply, the consumer, after having invited the trader to

15 DCD, art 3(1) and CC, art 135-*octies*(3) and (4); where, *ex* DCD, art 2(1) and (2) and CC, art 135-*octies*(2)(a) and (b), ‘digital content means data which are produced and supplied in digital form’ – such as music files, films, games or applications – and ‘digital service means (a) a service that allows the consumer to create, process, store or access data in digital form’ – such as cloud computing – or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service’ – such as social networks.

16 DCD, art 3(8); CC, art 135-*novies*(6).

17 DCD, recital n 12 and CC, art 135-*octies*(1).

18 DCD, art 7 and CC, art 135-*decies*(4).

19 DCD, art 8(1) and CC, art 135-*decies*(5).

20 DCD, art 8(2) and CC, art 135-*undecies*(1).

21 The action for conformity defects shall be time-barred within twenty-six months from the date of supply if the defects are apparent within that period: CC, art 135-*quaterdecies*(1), (2), (3) and (4).

22 Moreover, the burden of proof that the digital content or digital service was in conformity with the contract at the time of supply shall be on the trader for a lack of conformity that becomes apparent within a period of one year from the time the digital content or digital service was supplied: DCD, art 12 and CC, art 135-*sexiesdecies*.

supply the digital content or digital service, if the latter again fails to supply it, has the right to terminate the contract.²³ In the event of a lack of conformity, the consumer is entitled, first, to have the digital content or the digital service brought into conformity; second, he is entitled to a reduction in the price, proportional to the reduction in value, or to termination of the contract if: a) the remedy to bring the digital content or digital service into conformity is impossible or disproportionate; b) the trader has not restored the conformity within a reasonable time; c) a lack of conformity becomes apparent despite the trader's attempt to bring the digital content or digital service into conformity; d) the lack of conformity is so serious as to justify an immediate price reduction or termination of the contract; e) it appears that the trader will not bring the digital content or digital service into conformity within a reasonable time or without significant inconvenience to the consumer. With the clarification that the right to a price reduction only applies if the digital content or service is provided in exchange for the payment of a price – thus, not in exchange for personal data – and that, in this case, the consumer has no right to terminate the contract if the lack of conformity is minor.²⁴

In the event of termination of the contract, the trader is obliged to reimburse the consumer for all sums paid in performance of the contract and to comply with the obligations arising from Regulation (EU) 2016/679²⁵ (hereinafter, GDPR, General Data Protection Regulation).²⁶ Reimbursements due to price reduction or termination of the contract shall be carried out within fourteen days, using the same means of payment used by the consumer to pay, unless the consumer expressly consents to the use of another means.²⁷

Lastly, it should be noted that the Italian legislator, in implementing the DCD, has reproduced its provisions almost literally.

2. Critical aspects of the DCD in relation to contracts of

23 DCD, art 13(1) and CC, art 135-*septiesdecies*(1).

24 DCD, art 14 and CC, art 135-*octiesdecies*.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

26 DCD, art 16(1) and (2) and CC, art 135-*noviesdecies*(2) and (3).

27 DCD, art 18 and CC, art 135-*vicies*.

exchange between digital content or services and personal data

A brief exposition of the elements of the new discipline that are relevant to the ‘digital content/services versus personal data’ negotiation scheme highlights some of its many critical aspects.

Starting with the nature of personal data and the qualification of their provision. Indeed, the DCD (and, consequently, the Consumer Code) distinguishes between *contracts* where the trader supplies or undertakes to supply, a digital content or a digital service to the consumer and the consumer pays, or undertakes to pay, a price, and *where* the trader supplies, or undertakes to supply, digital content or a digital service to the consumer and the consumer provides, or undertakes to provide, personal data to the trader,²⁸ expressly excluding that personal data can be considered a commodity, comparable to a price.²⁹ Thus, the legislator poses the problem of the qualification of the act of provision of personal data – and, even before that, that of their nature – but does not solve it.³⁰

In addition, the DCD extends its scope of application to contracts for the exchange of digital content/services and personal data, thus generally extending the scope of consumer protection law to those involved in the relationships under consideration, defining, in fact, ‘consumer’ as ‘any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person’s trade, business, craft, or profession’.³¹ But having defined data subjects as consumers and having expressly referred to certain consumer protection regulations does not solve the problems of coordination between them and contracts in which, in exchange for the supply of a digital content or service, the consumer provides personal data.

Similarly, the DCD expressly provides the applicability – actually, the prevalence – of the Union law on the protection of personal data and, in particular, of the GDPR to any personal data processed in connection with contracts falling within its scope,³² without making any coordination between the various rules. Yet, certain provisions of the GDPR do not seem to fit well with the contracts under consideration, as well as with the DCD and the consumer protection laws.

28 DCD, art 3(1) and CC, art 135-*octies*(3) and (4).

29 DCD, recital n 24.

30 Camardi (n 14), 504.

31 DCD, art 2(6).

32 DCD, art 3(8); CC, art 135-*novies*(6).

3. Nature of personal data in the light of the opinions of the European Data Protection Supervisor and the Italian Competition Authority, legal scholars and case law

First of all, it is necessary to address the question of the nature of personal data, which logically precedes all other issues.

The Italian academic debate sees two opposing approaches: one is *protective*, aimed at limiting the data market, in order to protect the individual and his identity; the other is *liberalist*, aimed at liberalising the circulation of data, considered ‘goods’ with exchange value.³³ The first approach, traditionally accepted by scholars in this field,³⁴ emphasises the non-pecuniary and non-transferable nature of personality rights, excluding the possibility of transferring personal data.³⁵ In fact, personality rights have historically been characterised as inalienable, non-transferable, irretrievable and imprescriptible.³⁶ The second approach, which has spread in more recent times and prevails today,³⁷ assimilates personal data to assets in the legal sense, susceptible to being the subject of contractual provisions.³⁸

The DCD, as mentioned above, has not solved the problem. On the contrary, it has complicated it, having legalised the contractual scheme under consideration, but having, at the same time, excluded the reciprocal nexus between personal data and digital content/service.

It should be noted, however, that the text of the directive initially proposed by the Commission treated these contracts differently.³⁹ Indeed, recital n 13 stated that ‘In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money ie by giving access to personal data or other data. Those specific business models apply in different forms in a considerable

33 Guido Alpa, ‘La “proprietà” dei dati personali’, in Nadia Zorzi Galgano (ed), *Persona e mercato dei dati. Riflessioni sul GDPR* (Wolters-Cedam 2019), 13.

34 D’Ippolito (n 9), 643; Camardi (n 14), 507; Vincenzo Ricciuto, ‘La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno’, in Vincenzo Cuffaro, Roberto D’Orazio and Vincenzo Ricciuto (eds) (n 9), 26; Alberto De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Edizioni scientifiche italiane 2017), 12.

35 D’Ippolito (n 9), 643–644.

36 Andrea Torrente and Piero Schlesinger, *Manuale di diritto privato* (25th edn, Giuffrè 2021), 128.

37 D’Ippolito (n 9), 636; Ricciuto (n 34), 23 ss.; De Franceschi, ‘Il “pagamento” mediante dati personali’ (n 9), 1381 ss.

38 Andrea Stazi and Francesco Corrado, ‘Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica’ [2019] *Diritto dell’informazione e dell’informatica* 443, 457–458.

39 European Commission, ‘Proposal for a Directive on certain aspects concerning contracts for the supply of digital content’, COM (2015) 634 final.

part of the market. Introducing a differentiation depending on the nature of the counter-performance would discriminate between different business models; it would provide an unjustified incentive for businesses to move towards offering digital content against data. A level playing field should be ensured'. Consequently, art 3 identified the scope of application of the DCD in 'any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data'.

The reasons for the drastic change of course are to be found in the opinion of the European Data Protection Supervisor on the proposed directive, adopted on 14 March 2017,⁴⁰ which, while welcoming the initiative to protect consumers who do not pay a monetary price, emphasises that 'fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity'. Coherently, therefore, with the *protective* approach.

The Italian Competition Authority (hereinafter, AGCM, *Autorità Garante della Concorrenza e del Mercato*), on the contrary, takes a different view. In the proceedings initiated against WhatsApp Inc. for the alleged unfairness of certain clauses in the contractual model submitted for acceptance by consumers wishing to use the WhatsApp Messenger application, it stated that 'for the purposes of classifying the relationship established between WhatsApp and the consumer as contractual and of assessing the unfairness of the relevant clauses [...], it is of no significance that the services are provided without monetary consideration', because, 'personal data, consumer preferences and other user generated content, have a "de facto" economic value and are being sold to third parties', as argued by the European Commission in the document containing guidelines for the implementation of the Unfair Commercial Practices Directive.⁴¹

The AGCM expressed the same opinion in a case against Facebook, in which it found that: on the one hand, the companies Facebook Inc. and Facebook Ireland Ltd. did not adequately and immediately inform consumers, during the account activation phase, of the activity of collecting, with commercial intent, their data, inducing them to register on the platform, also emphasising the gratuity of the service; on the other hand, they exercised undue influence

40 European Data Protection Supervisor Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content [2017].

41 AGCM, Decision CV154, 11 May 2017, para 62, which refers to European Commission Staff Working Document Guidance On The Implementation/Application Of Directive 2005/29/EC On Unfair Commercial Practices Accompanying The Document Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses [2016] SWD (2016) 163 final.

on registered consumers, who suffer, without express and prior consent, the transmission and use by Facebook and third parties, for commercial purposes, of their data.⁴² This gave rise to two separate unfair commercial practices, respectively, misleading, under arts 21 and 22 CC, and aggressive, under arts 24 and 25 CC.⁴³ In particular, the AGCM justified the existence of a consumer relationship between Facebook and its users, and, therefore, the applicability of the Consumer Code, in consideration of the nature of non-pecuniary counter-performance of users' data. Which was confirmed in the *Facebook/Whatsapp* case by the Commission, where, in examining the competition profiles of Facebook's acquisition of WhatsApp, it stated that 'the vast majority of social networking services are provided free of monetary charges. They can however be monetized through other means, such as advertising or charges for premium services'.⁴⁴

The decision was challenged before the Regional Administrative Tribunal (hereinafter, TAR, *Tribunale Amministrativo Regionale*) of Lazio by both Facebook Ireland and Facebook Inc., *inter alia*, on the grounds of absolute lack of attribution by the AGCM, since: (a) it would not be a commercial practice in the absence of pecuniary consideration and (b) the discipline to be applied would be exclusively privacy legislation on the basis of the principle of speciality set out in art 3(4) of the Unfair Commercial Practices Directive.⁴⁵ However, according to the TAR, which upheld in part both appeals by annulling the decision of the AGCM in relation to the second contested practice, 'this approach suffers from a biased view of the potentialities inherent in the exploitation of personal data, which may also constitute an "asset" available in a contractual sense, susceptible to economic exploitation and, therefore, capable of assuming the function of "counter-performance" in the technical sense of a contract. In addition to the protection of personal data as the expression of an individual's personality right, and thus subject to specific and unwaivable forms of protection, such as the right to withdraw consent, access, rectification, and to be forgotten, there is also a different field of protection of the data concerned, considered as the

42 AGCM, Decision 27432, 29 November 2018, paras 70–71.

43 Discipline introduced by Italian Legislative Decree No 146/2007, implementing European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

44 AGCM, Decision 27432, 29 November 2018, para 54, which refers to European Commission, Case M.7217 – Facebook/WhatsApp, Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004, para 47.

45 According to which: 'In the case of conflict between the provisions of this Directive and other Community rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects'.

possible object of a trade, both between market operators and between the latter and the interested parties. The phenomenon of the “patrimonialisation” of personal data, typical of the new digital markets economies, requires operators to comply, in the relevant commercial transactions, with those obligations of clarity, completeness and non-misleading nature of the information laid down by the legislation for the protection of the consumer, who must be informed of the exchange of services that underlies the signing of a contract for the use of a service, such as using a social network.⁴⁶ Therefore, the provisions of the GDPR and those on consumer protection ‘stand in terms of complementarity’.⁴⁷

The TAR qualifies personal data as ‘possible object of a trade’, thus, exchanged with an onerous contract – a purchase contract⁴⁸ – with corresponding obligations, as confirmed by art 3(1) DCD, where it is stated that personal data provided must not be ‘exclusively processed by the trader for the purpose of supplying the digital content or digital service’. The Tribunal, therefore, identifies the right that an individual has over his or her personal data as a proprietary right that, as such, is transferred to the other party in exchange for the provision of a service.⁴⁹

The two TAR judgments were challenged before the Consiglio di Stato (Council of State), which rejected them, stating that ‘the reproach addressed to the trader would consist in not having informed the user, who in this case is technically transformed into a “consumer”, when he makes his data available in order to be able to use for free the services offered by the FB companies, prior to this operation, in whose context the user continues to believe that the attainment of the advantages connected with access to the platform is free of charge, not being able, therefore, to recognise and realise that in return for the advantage an automatic profiling for commercial use takes place, which is not clearly and immediately indicated, at the time of the first access, as an inevitable consequence of providing data’: social networks, then, although they are presented as free, ‘clearly, they are not that free, ending up representing the

46 Twin judgments TAR Lazio, 10 January 2020, No 260 and TAR Lazio, 10 January 2020, No 261, para 6.

47 *ibid* para 8, according to which ‘the non-overlapping of the plans relating to the protection of privacy and consumer protection is inferred from the considerations made by the Court of Justice of the European Union, of 13 September 2018, in Joined Cases C 54/17 and C 55/17, in which it ruled that the consumer rules do not apply “only where provisions, other than those of Directive 2005/29, which regulate specific aspects of unfair business practices, impose on undertakings, in such a way as to leave them no margin for discretion, obligations which are incompatible with those laid down in Directive 2005/29”’.

48 Fabio Bravo, ‘La “compravendita” di dati personali?’ [2020] *Diritto di internet* 521, 535.

49 Beniamino Parenzo, ‘Dati personali come “moneta”. Note a margine della sentenza TAR Lazio n. 260/2020’ [2020] *Jus Civile* 1364, 1371–1372.

“consideration” of making an individual user’s personal data available for commercial purposes?⁵⁰

In other words, according to the Consiglio di Stato, it is not the personal data that is exchanged to access the service, but only its ‘making available’, the possibility of using it.⁵¹ But, in any case, both administrative courts recognise the counter-performance nature of personal data, while distinguishing the type of transfer contract.

The Corte di Cassazione (Court of Cassation), the Italian court of last resort, also dealt with contracts for the exchange of services and personal data, in relation to a newsletter service, where, in order to access it, consent for the processing of personal data was required, which would be used not only for the supply of the service, but also for sending promotional communications and commercial information by third parties. The decision relates to the conditions of freedom and specificity of the data subject’s consent, but, indirectly, for the first time,⁵² also recognises the category of contracts under consideration: ‘the legal system does not prohibit the exchange of personal data, but nevertheless requires that such an exchange must be the result of a full and in no way coerced consent’.⁵³ The Corte di Cassazione, therefore, although not directly ruling on the nature of personal data, acknowledged, to some extent, their nature as counter-performance.

In any case, European data protection law itself argues in favour of the patrimonial nature of personal data. Even the Directive 46/95/EC, in its first recitals, identified the free flow of personal data as necessary for the establishment and functioning of the internal market, in which the free movement of goods, persons, services and capital is ensured.⁵⁴ Furthermore, the article on the object of the directive expressly provided that Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection of fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.⁵⁵

50 Twin judgments Consiglio di Stato, 29 March 2021, No 2630 and Consiglio di Stato, 29 March 2021, No 2631, respectively, paras 9–10 and paras 8–9.

51 Beniamino Parenzo, “Sull’importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l’esistenza di uno scambio sotteso ai c.d. servizi digitali “gratuiti” [2021] *Diritto di Famiglia e delle Persone* 1457, 1460.

52 Fabio Bravo, “Lo “scambio di dati personali” nei contratti di fornitura di servizi digitali e il consenso dell’interessato tra autorizzazione e contratto” [2019] *Contratto e impresa* 34, 35.

53 Corte di Cassazione, 2 July 2018, No 17278, para 2.5.

54 Directive 95/46/EC European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, recital n 3.

55 Directive 95/46/EC, art 1.

Yet, among the objectives of the Italian law transposing the directive there was no reference to guaranteeing the free movement of personal data.⁵⁶ And also the so-called Italian Privacy Code,⁵⁷ which repealed the previous law implementing the directive, while providing for the free and non-restrictable circulation of personal data, placed the relevant provision outside the purpose of the law.⁵⁸ Probably because Italian legal scholars have long understood personal data in the sole sense of absolute subjective rights.⁵⁹

The contractual approach is much more evident in the GDPR, already in art 1: '(1) This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. (2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. (3) The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'. According to some, in fact, this provision puts the *personalist* approach – concerning the protection of natural persons with regard to the processing of personal data – and the *market* approach – concerning the free movement of personal data – on an equal footing⁶⁰ and, according to others, the second approach would even prevail over the first, since the third paragraph of the provision changes the order of terms, placing the circulation of data in a super-ordinate position.⁶¹

Besides, the legal bases of the data subject consent⁶² and of the processing necessity for the performance of a contract⁶³ seem to confirm the contractual

56 Italian Law No. 675/1996, art 1(1), according to which 'This law guarantees that the processing of personal data is carried out with respect for the rights, fundamental freedoms and dignity of natural persons, with particular reference to privacy and personal identity; it also guarantees the rights of legal persons and any other body or association'.

57 Italian Legislative Decree No. 196/2003, which entirely reorganised the subject of personal data protection due to the regulatory complexity created by the approval of various rules in this field.

58 Compare Italian Legislative Decree No. 196/2003, arts 2(1) ('[...] the "Code", ensures that the processing of personal data is carried out with respect for the fundamental rights and freedoms, as well as for the dignity of the data subject, with particular reference to privacy, personal identity and the right to protection of personal data) and 42 ('The provisions of this Code may not be applied in such a way as to restrict or prohibit the free movement of personal data between the Member States of the European Union, without prejudice to the adoption, in accordance with the same Code, of any measures in the event of transfers of data carried out in order to circumvent those provisions').

59 Ricciuto (n 34), 26–33.

60 Ricciuto (n 34), 53; D'Ippolito (n 9), 656.

61 Parenzo, 'Sull'importanza del dire le cose come stanno' (n 51), 1465.

62 GDPR, art 6(1)(a).

63 *ibid* art 6(1)(b).

nature of the processing of personal data.⁶⁴ The same is true for the right to data portability and, in particular, for the provision that, where the processing is based on consent or contract and is carried out by automated means, the data subject shall have the right to have his or her personal data transmitted directly from one controller to another, where technically feasible:⁶⁵ such a claim can only fall within the concept of obligation, requiring the data controller to perform in satisfaction of an interest of the data subject, in addition, only in relations based on consent or contract and, therefore, interindividual.⁶⁶

In the light of the reconstruction carried out on the basis of European data protection legislation, as well as Italian case law and legal scholars, the dual nature of personal data cannot be denied: on the one hand, personal data as the expression of a personality right and, on the other, as the counter-performance of the supply of a service, which therefore cannot be said to be free of charge. Besides, recognising the patrimonial nature of personal data and classifying the contracts with which they are exchanged as onerous contracts enables the natural person to understand how access to certain services is not without consequences,⁶⁷ while also protecting him as a consumer.

Still, as mentioned above, the DCD stands in contrast to this picture. Nevertheless, the fact that the DCD does not qualify as contracts those relations in which personal data are provided in exchange for a service, denying their nature as commodities, does not imply that such transactions cannot be qualified as synallagmatic contracts.⁶⁸ Indeed, not only does the description of the economic transaction confirm the possibility of considering the providing of personal information as a contractual service,⁶⁹ but, above all, it is a purely nominalistic matter, since the rules governing these relations are the same as those governing contracts in which a monetary consideration is envisaged.⁷⁰ In any case, it is undeniable that this dichotomy creates serious problems of interpretation and, above all, application, which can only be solved by the European legislator.

One point still remains to be clarified, however: whether it is the personal data that are transferred with the contract or is it rather a transfer of the enjoyment of them, although most commentators seem to rule out the configurability of a contract of sale, as the data subject does not lose control over his or her personal data, which, in fact, he or she may also make available to other

64 Ricciuto (n 34), 54 ss.; D'Ippolito (n 9), 656.

65 GDPR, art 20(2).

66 Ricciuto (n 34), 45-46.

67 Parenzo (n 51), 1466-1467.

68 *ibid* 1487.

69 Roberto Senigaglia, 'La dimensione patrimoniale del diritto alla protezione dei dati personali' [2020] *Contratto e impresa* 760, 766.

70 Shaira Thobani, 'Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente' [2019] *MediaLaws* 131, 146.

controllers.⁷¹ This will lead to the qualification of this contract and its legal consequences, which, as said, are left to the Member States.

But apart from that, three levels of protection now apply to the contracts under examination: consumer protection – applied, in fact, by the AGCM, TAR and Consiglio di Stato in relation to unfair commercial practices –, data protection – expressly referred to in the DCD – and contractual protection.⁷²

4. Coordination problems with consumer protection law: pre-contractual information and unfair commercial practices

The DCD recognises that the data subject whose data are processed in a contract for the provision of a digital content or service is considered a consumer. A consumer to whom, therefore, consumer protection law shall generally apply. Yet, the directive does not coordinate its content with consumer protection legislation, which is particularly evident and problematic in relation to pre-contractual information and unfair commercial practices.

Starting with pre-contractual information, recital n 42 DCD states that: ‘The digital content or digital service should comply with the requirements agreed between the trader and the consumer in the contract. [...] The requirements of the contract should include those resulting from the pre-contractual information which, in accordance with Directive 2011/83/EU, forms an integral part of the contract [...]’. Thus, under the DCD, the requirements for contracts governed by it also include the pre-contractual information set out in the Directive 2011/83/EU,⁷³ transposed in Italy in the CC.⁷⁴

In particular, if the relationships under consideration were to be considered contracts, as we have argued so far, they would fall within the definitions of

71 *Ex multis*, Parenzo (n 51), 1468–1469; Bravo (n 48), 535 ss.; Stazi and Corrado (n 36), 464 ss.; Ricciuto (n 34), 48.

72 Bravo (n 48), 534.

73 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64, recently amended by Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements, amending Regulation (EC) No 2006/2004 and Directive 2011/83/EU of the European Parliament and of the Council and repealing Council Directive 90/314/EEC [2015] OJ 326/1 and Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7.

74 CC, art 45 ss.

‘service contract’, that is any contract other than a sales contract under which the trader supplies a service to the consumer and the consumer pays the price,⁷⁵ and of ‘distance contract’, that is any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded.⁷⁶

For these types of contracts, the Directive provides that, before the consumer is bound by a distance contract or any corresponding offer, the trader shall inform the consumer in a clear and comprehensible manner of the total price of the goods or services.⁷⁷ Furthermore, if the distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the total price and the trader shall ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay. Otherwise, the consumer shall not be bound by the contract or order.⁷⁸

However, the Directive does not provide any definition of ‘price’ or ‘payment’. Some suggest, also in the light of the DCD, that these concepts should be interpreted in an evolutionary way, not limiting them to obligations involving the transfer of money, but encompassing all services having economic value, including those involving the exchange of personal data: after all, the Italian Civil Code uses the terms ‘payment’ and ‘performance’ indistinctly. It would follow that whenever a trader presented a service as free of charge, neither the contract for the supply of digital services nor the order issued by the consumer would be binding.⁷⁹

With regard to unfair commercial practices, the Directive 2005/29/EC and the CC state that a commercial practice shall be regarded as misleading if it contains false information, deceives or is likely to deceive the average consumer or omits material information, also in relation to the price to be paid, causing him to take a transactional decision that he would not have taken otherwise.⁸⁰ Therefore, offering a contract for free, which, in reality, is for consideration, as it implies the providing of personal data, constitutes a misleading unfair commercial practice, having induced consumers to take a commercial decision they would not otherwise have taken, namely to register on the social network, via

75 Directive 2011/83/EU, art 2(6) and CC, arts 45(f) and 46(1).

76 Directive 2011/83/EU, art 2(7) and CC, art 45(g).

77 Directive 2011/83/EU, art 6(1)(e) and CC, art 49(1)(e).

78 Directive 2011/83/EU, art 8(2) and CC, art 51(2).

79 De Franceschi (n 9), 1391–1394.

80 Directive 2005/29/EC, arts 6(1)(d) and 7(1); CC, arts 21(1)(d) and 22(1).

website or app, and to remain in it, as found by the AGCM, TAR and Consiglio di Stato.⁸¹

Part of the legal scholars also believe that if an unfair commercial practice is found to exist, consumers are entitled to compensation for the resulting pecuniary loss and may also file a class action.⁸²

The dangerous impact that considering the exchange of services and personal data as an onerous contract could have is, hence, evident. Nevertheless, the path taken by Italian legal scholars and case law seems to be moving in this direction, thus making it difficult to reconcile the already existing consumer discipline with these contracts and leaving major interpretative and applicative doubts unresolved.

5. Coordination problems with GDPR: nature, freedom and withdrawal of consent and conformity requirements

The problem of coordination between the DCD and other legislation does not only concern consumer law, but also and above all data protection law. And, in particular, the GDPR, which the European legislator merely referred to, although some issues would have deserved clarification.

First of all, it is not specified what are the conditions of lawfulness on which the processing under the contract in question can be based, however this can be deduced from the DCD. Indeed, as mentioned before, the DCD applies where the trader supplies digital content or service and the consumer provides personal data, ‘except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose’.⁸³ The last two exceptions evidently refer to the hypotheses provided for in letters b) and c) of art 6(1) GDPR, ie where the processing of personal data is necessary for the performance of a contract to which the data subject is party or for compliance with a legal obligation to which the controller is subject. Thus, the only legal basis that seems to be able to justify such processing is consent⁸⁴. But it is unclear whether consent coincides with contractual consent, whether it is compatible with data protection law, and what happens if consent is withdrawn.

81 AGCM, Decision 27432, 29 November 2018, para 70; twin judgments TAR Lazio, 10 January 2020, No 260 and TAR Lazio, 10 January 2020, No 261, para 13; twin judgments Consiglio di Stato, 29 March 2021, No 2630 and Consiglio di Stato, 29 March 2021, No 2631, respectively, paras 11 and paras 10.

82 De Franceschi (n 9), 1402–1403.

83 DCD, art 3(1) and CC, art 135-*octies*(4).

84 GDPR, art 6(1)(a).

The first problem relates to the nature of the consent to the processing of personal data – which is closely related to the issue of the qualification of personal data discussed above –: Italian legal theory is divided between those who attribute to it a contractual nature and those who qualify it as a legal act, comparable to a justification or an authorisation.⁸⁵ According to the former, consent constitutes the expression of will with regard to the circulation of personal data.⁸⁶ According to one part of the latter, the processing of personal data is *per se* unlawful and the consent of the data subject excludes unlawfulness;⁸⁷ according to the other part, on the contrary, the processing is *per se* lawful and the consent intervenes just to remove a limitation that the law places on the power of the data controller.⁸⁸

In the aforementioned judgment, the Corte di Cassazione stated that it is ‘to be excluded that the consent considered by this provision [ie, art 23 of the Italian Privacy Code⁸⁹] is simply the same consent in general required for contractual purposes’;⁹⁰ part of the scholars has, therefore, deemed it necessary to have a double consent, one for the conclusion of the contract and one for the processing of personal data.⁹¹ However, a large part of the scholars remains convinced of the opposite theory, due in part to the judgments of the TAR and the Consiglio di Stato, which, by recognising the contractual nature of personal data or, at least, of their provision, lead to reconstructing consent in contractual terms. The debate, therefore, still remains open.

In any case, even assuming that consent for contracts involving the exchange of personal data is unique, such consent should comply with the GDPR, according to which “‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.”⁹² It is precisely the requirement of freedom of consent that could create problems in relation to the

85 Parenzo (n 49), 1374.

86 Ricciuto (n 34), 56.

87 Ilaria Amelia Caggiano, ‘Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali’ [2018] Osservatorio del diritto civile e commerciale 67, 84 ss.

88 Bravo (n 52), 42 ss.

89 Now repealed, according to which: ‘1. The processing of personal data by private individuals or public economic entities is only permissible with the express consent of the person concerned. 2. Consent may relate to the entire processing or to one or more of its operations. 3. Consent shall only be validly given if it is freely and specifically expressed with reference to a clearly identified processing operation, if it is documented in writing, and if the information referred to in Article 13 has been provided to the data subject. 4. Consent shall be given in writing when the processing relates to sensitive data’.

90 Corte di Cassazione, 2 July 2018, No 17278, para 2.4.

91 Bravo (n 52), 40 ss.

92 GDPR, art 4(11).

contracts under consideration, in respect of which the GDPR provides additional guidance, stating that ‘when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract’.⁹³

It is, therefore, not forbidden to make the performance of a contract conditional on the provision of consent to the processing of data, although this circumstance must be taken into *utmost* account. This article has been interpreted by the European Data Protection Authorities, with reference precisely to those situations of “tying” the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service’.⁹⁴ And, although the article is not construed in an absolute manner, they argued that ‘there might be very limited space for cases where this conditionality would not render the consent invalid’.⁹⁵

More specifically, to make this assessment, according, first, to the Article 29 Working Party and, then, to the European Data Protection Board (EDPB), consideration must be given to the fact that ‘the element “free” implies real choice and control for data subjects’;⁹⁶ the *reality* of the choice depends on the possibility for the data subject to access the service even without giving consent and, thus, presupposes that the provider offers two versions of the same service, one conditional on consent and the other one not. Moreover, ‘both services need to be genuinely equivalent’.⁹⁷

In any case, they exclude the freedom of consent ‘if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand’;⁹⁸ in such a scenario, freedom of choice would depend on other market participants and on subjective judgments of equivalence, while obliging data controllers to monitor the market to ensure the continued validity of consent in case a competitor changes its service.

Accepting this interpretation would end up considering the consent as invalid and, therefore, the processing provided for the large and growing number of

93 *ibid* art 7(4).

94 Article 29 Working Party Guidelines on consent under Regulation 2016/679 [2017] 17/EN WP259 (Article 29 WP Guidelines Consent), 8; EDPB Guidelines on consent under Regulation 2016/679 [2020] 05/2020 (EDPB Guidelines Consent), para 26.

95 Article 29 WP Guidelines Consent, 9; EDPB Guidelines Consent, para 35.

96 Article 29 WP Guidelines Consent, 5; EDPB Guidelines Consent, para 13.

97 Article 29 WP Guidelines Consent, 9; EDPB Guidelines Consent, para 37.

98 Article 29 WP Guidelines Consent, 9–10; EDPB Guidelines Consent, para 38.

tying contracts as unlawful. However, both Italian case law and academia deviate from this view.

When it comes to case law, it suffices to cite the administrative judgments on unfair commercial practices: while recognising profiles of unlawfulness within *tying* operations, their validity was indirectly recognised. In addition, the Corte di Cassazione, in the aforementioned judgment, also showed a favorable view, stating that, when assessing whether consent is freely given, ‘conditioning cannot always and in any case be taken for granted and should instead be deemed to exist the more the service offered by the provider of the Internet site is at once non-fungible and indispensable for the data subject’,⁹⁹ where ‘non-fungible’ refers to the possibility of access to similar services and ‘indispensable’ to the importance of the service for the user.

As for the academia, it was first noted that the validity of consent is to be assessed at the time it is given, so it is irrelevant that the service provided by another market participant changes, also because the data subject could withdraw it in any case. Moreover, there is no reason to consider the requirement of equivalence between different services as subjective, adopting an objective notion of equivalence linked to their characteristics. Thus, consent given against an alternative, provided by the same or other operators, is considered free, in line with the Corte di Cassazione’s ruling.¹⁰⁰

However, it has been pointed out that, if a service is fungible, it is, as such, also renounceable, but the same cannot be said for a non-fungible service. The Facebook example is emblematic: the service offered by Facebook is probably non-fungible, as there are no real equivalents on the market, but it cannot be called essential and indispensable. It seems, however, preferable to reserve the qualification of renounceable only for the most futile cases and to consider that non-fungible services are also indispensable.¹⁰¹

The distinctiveness of consent to data processing lies not only in the specific validity requirement mentioned above, but also in the provision for its revocability: on the one hand, the right to withdraw consent presents significant coordination problems with Directive 2011/83/EU in relation to the exceptions to the right of withdrawal from a distance contract, and, on the other hand, it raises several doubts in relation to restitution obligations or reimbursements.

In the first place, under the GDPR, the data subject shall have the right to withdraw his or her consent at any time: this is an unwaivable right.¹⁰² But, at the same time, the Directive 2011/83/EU and the CC provides that the right of withdrawal for distance contracts – which, as noted above, includes the contracts under consideration – is excluded with respect to contracts for the supply

⁹⁹ Corte di Cassazione, 2 July 2018, No 17278, para 2.5.

¹⁰⁰ Thobani (n 70), 142.

¹⁰¹ *ibid* 143.

¹⁰² GDPR, art 7(3).

of digital content which is not supplied on a tangible medium, if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal.¹⁰³ This was intended to prevent the consumer from abusing the right of withdrawal by exercising it and demanding the return of the service received, after obtaining and storing the digital content. However, this exception to the right of withdrawal from a distance contract will not be applicable if the counter-performance consists of personal data, since such a waiver would be incompatible with the GDPR: this inapplicability is likely to create unequal treatment between payment by means of a sum of money and payment by means of personal data.¹⁰⁴

In the second place, where the right of withdrawal is exercised, the right to regulate its consequences is left, as mentioned above, to the Member States. Which poses, first of all, coordination problems between States, in a context where digital content or service providers operate globally, without geographic boundaries. The major problem, however, concerns the qualification of the contracts under consideration – which, as has been amply exposed, is far from being resolved –, so that the rules relating to that particular type of contract can be applied. But in any event, even if the contracts under consideration were recognised as belonging to a certain type, that type would certainly not have provisions that take account of their peculiarities, constituting a *unicum* in the contracts expressly regulated today. And, furthermore, should the termination of the contract result, according to the law of a Member State, in the full restitution of the services performed and, therefore, in the restitution of the personal data as well, it is difficult to imagine how this could be achieved. Indeed, by the time the data subject withdraws consent to processing, the person who received them, the trader, will already have made a financial profit and, as a consequence of their further disposal, will also, usually, have already lost track of them. In this regard, it has also been pointed out that monetary compensation in such a case may be difficult to quantify.¹⁰⁵

Finally, another coordination issue between the GDPR and the DCD concerns the conformity requirements of the latter. In this respect, in fact, there is a discrepancy between the recitals – where it is provided that ‘facts leading to a lack of compliance with requirements provided for by Regulation (EU) 2016/679, including core principles such as the requirements for data minimisation, data protection by design and data protection by default, may, depending on the circumstances of the case, also be considered to constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity provided for in this Directive’¹⁰⁶ – and the articles

103 Directive 2011/83/EU, art 16(m) and CC, art 59(1)(o).

104 De Franceschi (n 9) 1408.

105 *ibid* 1407.

106 DCD, recital n 48.

of the DCD – where there is no reference to compliance of the content or service with the GDPR.

Despite this, it is argued that GDPR compliance requirements are included in the objective requirements for conformity of art 8 DCD, according to which the digital content or digital service shall ‘be fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, where applicable, any existing Union and national law, technical standards or, in the absence of such technical standards, applicable sector-specific industry codes of conduct’ and shall ‘possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect, given the nature of the digital content or digital service’.¹⁰⁷

The reference to average quality standards, in fact, can only refer also to those imposed by the GDPR, given the oft-mentioned provision of the prevalence of the data protection law over the DCD,¹⁰⁸ as well as the provision according to which in the event of termination of the contract the trader shall comply with the obligations applicable under the GDPR:¹⁰⁹ it would be contradictory not to give the consumer contractual remedies when the GDPR rules are violated.¹¹⁰

However, this is an issue that, like the previous ones, would have deserved a clarifying intervention by the legislator and not a generic reference to the GDPR.

6. Findings

An attempt has been made, here, to reconstruct (part of) the debate created around the figure of contracts for the exchange of digital content or services and personal data. Debate still characterized by great ferment and difference of views, not reconciled and, indeed, further distanced by the DCD.

The purpose of this paper, in fact, was to retrace the critical issues generated by having recognised these contracts in a European legislative text, without claiming to find a solution, but in order to show how having expressly differentiated them from contracts in which a price is paid in money has created more problems than it has solved.

Above all, because, although there is no express qualification of personal data and of the contracts under which they are put into circulation, it is now undisputed that three levels of protection apply to them: consumer protection,

107 DCD, art 8(1)(a) and (b) and CC, art 135-*decies*(5)(a) and (b).

108 DCD, art 3(8); CC, art 135-*novies*(6).

109 DCD, art 16(2) and CC, art 135-*noviesdecies*(3).

110 Camardi (n 14) 513–520.

personal data protection and contractual protection. And each of these sets of provisions is not only unsuitable for these contracts, but it is not even clear how it applies. With the risk, moreover, that each level continues to be regulated independently of the others and, above all, without provisions appropriate to the contracts under consideration: bringing forward all three levels separately would create insurmountable coordination problems.

While it is true that an express recognition of this contractual scheme in European legislation is an important achievement, it is also true that the legislator has not fully achieved the objectives it set with the first recitals of the DCD: ‘consumers should benefit from harmonised rights for the supply of digital content and digital services that provide a high level of protection. They should have clear mandatory rights when they receive or access digital content or digital services from anywhere in the Union. Having such rights should increase their confidence in acquiring digital content or digital services. It should also contribute to reducing the detriment consumers currently suffer, since there would be a set of clear rights that will enable them to address problems they face with digital content or digital services’.¹¹¹

Yet, it cannot yet be said to exist a ‘a set of clear rights’ enabling consumers to address problems they encounter with digital content or digital services obtained in exchange for their personal data. Some significant examples have been given so far.

We can only hope that the legislator will again intervene on the issue, removing the ‘the major obstacles to the development of cross-border e-commerce in the Union [...]’. Ensuring better access for consumers to digital content and digital services, and making it easier for businesses to supply digital content and digital services, can contribute to boosting the Union’s digital economy and stimulating overall growth’.¹¹²

111 DCD, recital n 8.

112 *ibid* recital n 1.

A Lifeguard in Times of Pandemic: Electronic General Meetings in Joint Stock Companies

*Ufuk Tekin **

Eskişehir Osmangazi University, Faculty of Law, Turkey

ORCID 0000-0001-7823-1456

DOI: 10.54103/milanoup.215.c455

Abstract

The general meetings of joint stock companies are mandatory and a platform established by law for shareholders, directors and other stakeholders in these companies to make decisions, share information and opinions to move the company forward. These meetings of joint stock companies were also affected from COVID-19 outbreak measures. Within this framework, the general meetings of joint stock companies planned to be held during the pandemic have been postponed or held electronically within the scope of these measures. In this study, it is discussed whether the holding of joint stock company general meetings electronically can be considered as a permanent solution in extraordinary circumstances such as pandemic that may occur in the future. For this purpose, it has been discussed whether the provision 118a, which was added to the German Stock Corporation Act in July 2022, would be taken as an example, and in this respect, the literature on German law has been reviewed and these studies have been referred to. Also, due to the American origin of electronic general meetings, the literature on American law has also been benefited from. Since Turkish company law is influenced by German law, a comparison with Turkish law has also been made and Turkish doctrine on this subject has also been used.

Keywords

Joint Stock Company, General Meeting, Electronic General Meeting, Online General Meeting, Virtual General Meeting

* Eskişehir Osmangazi University, Faculty of Law, Commercial Law, utekin@outlook.com.tr, ORCID: 0000-0001-7823-1456. This study is based on the author's thesis titled "Electronic decision making and meeting principles of general assembly of limited liability company".

1. Introduction

The general meetings of joint stock companies are mandatory and a platform established by law for shareholders, directors and other stakeholders in these companies to make decisions, share information and opinions to move the company forward. These meetings of joint stock companies were also affected from COVID-19 outbreak measures. Within this framework, the general meetings of joint stock companies planned to be held during the pandemic have been postponed or held electronically within the scope of these measures.¹ In this study, it is discussed whether the holding of joint stock company general meetings electronically can be considered as a permanent solution in extraordinary circumstances such as pandemic that may occur in the future.

2. The usage of electronic platforms in general meetings

2.1. Advantages

Developments in technology have made it inevitable for the commercial life to keep pace with these advances. As a result of this, electronic platforms, which can be described as an alternative to classical shopping and marketing methods, have emerged with the possibility of electronic e-commerce. Technological developments have also affected corporate law, and it has been discussed whether the general meetings of joint stock companies should be held electronically. As a result of these discussions, general meetings started to be held electronically in various States, especially Delaware (in 2000),² and this was followed by EU countries with the effect of Directive 2007/36/EC.³ The reasons for pushing countries to hold general meetings electronically are various. One of the most important of these reasons is that if the shareholders are required to physically attend the general meetings, they will not be able to play an effective role in the

1 For detailed information on the situation before the pandemic and the measures adopted by various countries during the pandemic, also see: Dirk A. Zetzsche, Linn Anker-Sørensen, Roberta Consiglio and Miko Yeboah-Smith, 'COVID-19-Crisis and Company Law – Towards Virtual Shareholder Meetings – (2020) <<https://ssrn.com/abstract=3576707>> accessed on 8 February 2023, 10–25.

2 Lisa M. Fairfax, 'Virtual Shareholder Meetings Reconsidered' (2010) 40 Seton Hall Law Review 1367, 1368; Yaron Nili and Megan Wischmeier Shaner, 'Virtual Annual Meetings: A Path toward Shareholder Democracy and Stakeholder Engagement' (2022) 63 Boston College Law Review 123, 155.

3 Directive 2007/36/EC of the European Parliament and of the Council of 11 July 2007 on the exercise of certain rights of shareholders in listed companies [2007] OJ L 184.

decision-making mechanism of the company due to the extremely low attendance and as a result, the possible power gaps in the company.⁴

The power gap is caused by the fact that shareholders, who have very little opportunity to influence the management of the company since the ratio of their shares to the capital is very low, do not want to participate in the management, expect only to gain profit from the investment and thus alienate themselves from the company.⁵ Indeed, since the non-attendance of the shareholders to the general meetings may cause them not to have an idea about the activities of the company, as well as not being able to express their opinions, criticise and vote, it is obvious that this situation will adversely affect the functioning of the company.⁶ By holding the meetings electronically, it is aimed to eliminate the expenses such as travelling and accommodation that shareholders will incur in order to attend the meeting and to prevent them from not attending the general meetings due to the time they will lose or because they are unaware of the meeting, and thus to ensure effective participation by establishing shareholder democracy.⁷

Since the electronic participation to the general meetings will reduce the loss of time and enable shareholders to communicate with each other without requiring much expense, the attendance to these meetings will be extremely high.⁸ In this way, communication between shareholders will increase, and shareholders will be informed about the progress of the company by reviewing annual reports and meeting documents.⁹ In addition, since it is the duty of the general

-
- 4 Ünal Tekinalp, *Halka Açık Anonim Ortaklıklarda Yönetime Katılma Sorunları* [1979] İstanbul University, 7; Mehmet Emin Bilge, 'Anonim Ortaklık Genel Kurul Toplantılarında Temsilci Aracılığıyla Oy Vermede İnternetin Kullanımı' (2003) 7 Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi 341; Mustafa İsmail Kaya, 'Anonim Ortaklıkların Genel Kurul Toplantılarının İnternet Aracılığıyla Yapılması' (2003) 52 Ankara Üniversitesi Hukuk Fakültesi Dergisi 212.
 - 5 Işık Özer, 'Türk Ticaret Kanunu Tasarısına Göre Anonim Şirket Genel Kuruluna Elektronik Ortamda Katılım' (2009) 25/4 Banka ve Ticaret Hukuku Dergisi 621, 628.
 - 6 George Ponds Kobler, 'Shareholder Voting Over the Internet: A Proposal for Increasing Shareholder Participation in Corporate Governance' (1997-1998) 49 Alabama Law Review 673, 675-676.
 - 7 Lisa M. Fairfax, 'The Future of Shareholder Democracy' (2009) 84 Indiana Law Journal, 1259, 1260-1308; Özer (n 5) p. 627; Bilge (n 4) 341; Arthur R. Pinto, 'The European Union's Shareholder Voting Rights Directive From an American Perspective: Some Comparisons and Observations' (2008-2009) 32 Fordham International Law Journal, 489, 608; Kobler (n 6) 699-700; Daniel Adam Birnhak, 'Online Shareholder Meetings: Corporate Law Anomalies or The Future of Governance?' (2003) 29 Rutgers Computer&Technology Law Journal 423.
 - 8 Caspar Rose, 'The New European Shareholder rights directive: Removing Barriers and Creating Opportunities for More Shareholder Activism and Democracy' (2010) Journal of Management & Governance 269, 277; Joanna Kulesza, 'International Internet Law' (2012) 24 Global Change, Peace&Security 351, 357-359.
 - 9 Ralf Isenmann and Christian Lenz, 'Customized Corporate Environmental Reporting by Internet-Based Push and Pull Technologies' (2001) 8 Eco-Management and Auditing 100, 101; Kobler (n 6) 677.

assembly to appoint and dismiss managers, by ensuring the effective participation of shareholders in the decision-making process, managers, who may be dismissed at any time, will play an active role in increasing the value of the company in the macro sense by managing the company better with this concern.¹⁰ One of the important contributions of electronic attendance to the general meetings is that it enables these meetings to be held in extraordinary periods such as pandemics, when it is not possible for shareholders to physically attend, and thus enables the company to continue its operations.

2.2. Disadvantages

It should be noted that there are some disadvantages as well as advantages of electronic participation in the general meetings. The biggest problem arising from the electronic participation in the general meetings arises from the fact that the shareholders cannot meet face to face. That is to say, shareholders who are not physically meet are deprived of the opportunity to influence each other with their opinions, gestures and mimics and gain favour by participating in the general meetings electronically.¹¹ Physical communication will be replaced by communication through computers, which will lead to the replacement of human relations with technology and a decrease in communication between individuals. In addition, although the shareholders who attend the general meeting electronically may have the opportunity to follow the meeting via technical means, they may also experience a trust problem towards the company with the belief that confidential relations are carried out behind closed doors.

The high level of participation desired through electronic attendance to the general meetings may also become a disadvantage. Namely, if the effective participation of shareholders in the decision-making mechanism of the company by expressing their opinions and votes exceeds the limits of proportionality, unnecessary discussions and contradictions of opinion may lead the company to the point of not being able to take decisions.¹² Therefore, in the context of ensuring effective participation and shareholder democracy, which is aimed by electronic participation in the general assembly, the balance of interests should

10 Chris Mallin and Andrea Melis, 'Shareholder Rights, Shareholder Voting, and Corporate Performance' (2012) 16 *Journal of Management & Governance* 171, 173; Kobler (n 6) 687, 697; Blake Smith, 'Proxy Access and The Internet Age: Using Electronic Shareholder Forums to Improve Corporate Governance' (2008) 3 *Columbia Business Law Review* 1111, 1118; Birnhak (n 7) p 424.

11 Kaya (n 4) 222. On the grounds that this would alienate the shareholders from each other, also see: Julian Redeke, 'Virtuelle Hauptversammlungen börsennotierter Aktiengesellschaften "Virtual Insanity"?' (2022) *Die Aktiengesellschaft* 98, 100.

12 For a similar view also see: Klaus J. Hopt, 'Corporate Governance and the Shareholders: The German Law on Virtual General Meetings 2022' (2022) <<https://ssrn.com/abstract=4240280>> accessed on 8 February 2023, 4.

be well considered, and the company should not be pushed into insolvency instead of being a solution for it.¹³

It is clear that the electronic environment will enable shareholders to avoid unnecessary bureaucratic procedures and stationery due to the speed it provides. On the other hand, it is also possible that the shareholders are not aware of technological opportunities or do not have the ability to use them. Moreover, even if the shareholders are well-equipped in the use of the technological tools, sometimes it may not be possible to carefully evaluate gigabytes of images, sounds and other documents, and this may lead to erroneous decisions.¹⁴ In addition to the excessive amount of data, in the event of some technical problems such as interruption of the internet network connection, the flow of data may not be possible and shareholders may consider electronic participation undesirable.

Another problem related to electronic participation in general meetings is the reliability of such attendance. The exercise of rights such as the right to participate in the general meeting and the right to vote, which have a direct impact on the investments of shareholders, through the internet network via computers and technical components causes various question marks in the minds of those who exercise these rights: is the person who uses a vote really a shareholder, and is he/she able to use his/her vote securely? The solution for determining whether the voter is actually a shareholder can be provided by issuing a PIN (personal identification number) to the shareholders. Although there is always the concern that unauthentic shareholders may vote by unlawfully obtaining the PIN, the possibility of identification through various biometric indicators will significantly reduce these concerns. The problem of secure voting is relatively more difficult to solve. Indeed, while the internet is extremely useful in some respects, it is also extremely vulnerable to cyber-attacks. In such a situation, it is possible to say that cyber-attacks can be greatly reduced, if not completely eliminated, by ensuring network security by experts.

3. Types of electronic participation

It is possible to classify the general meetings of joint stock companies in various aspects. Since this study is related to electronic meetings, the types to be examined under this heading differ depending on the extent to which the general meeting is held electronically. Namely, holding general meetings entirely in electronic environment is referred to as virtual general meetings, while the

13 Kobler uses digital cacaphony for such situations, (n 6) 696; Mehmet Emin Bilge, 'Pay Sahiplerinin Anonim Ortaklık Genel Kurullarına İnternet Aracılığıyla Katılımı', (2003) Bilgi Toplumunda Hukuk, Ünal Tekinalp'e Armağan 219, 223.

14 Kobler (n 6) 687.

ability of shareholders to attend physical general meetings also in electronic environment is referred to as online general meetings. Although holding general meetings virtually or online varies from country to country, it is seen that, especially after the pandemic, large countries such as Germany¹⁵ have started to hold their general meetings completely electronically in the form of virtual general meetings.

3.1. Virtual general meetings

In virtual general meetings, the general assembly is held entirely electronically.¹⁶ In other words, in a virtual general meeting, only the people who are obliged to attend for the administration of the meeting are required to attend, and shareholders are not required to be physically present at the location of these people. In fact, such general meetings are not general assembly in the classical sense, where shareholders physically come together at a specific time and place, but rather meetings that take place entirely electronically.¹⁷

Virtual general meetings are favoured because they are significantly less expensive in terms of time and cost. This is because such meetings allow shareholders to participate from wherever they are through their computers. It is clear that this situation will increase the participation of shareholders in the general assembly. However, this may always lead to undesirable results. In particular, as mentioned before, digital cacophony may occur and general meetings may become dysfunctional due to unnecessary interventions of shareholders.¹⁸ In such a case, limiting the rights of shareholders to actively participate in the meetings, such as expressing opinions and asking questions, for reasonable and certain periods of time, in a manner that does not violate equality among them, may be considered as a solution.¹⁹

Another argument put forward by opponents of virtual general meetings is whether the technology is suitable for this. However, considering the practices in almost all of the world between 2020 and 2022, it is possible to say that almost all areas of life have been moved to the electronic environment. The needs that emerged during the pandemic, when the physical relationship between people was minimised, paved the way for the development of new technologies. With the effect of this situation, systems that ensure the smooth

15 Recent developments in German law will be discussed in detail below.

16 Elizabeth Boros, 'Virtual Shareholder Meetings' (2004-2005) 3 *Duke Law&Tech Review* 1.

17 Bilge (n 13) 224.

18 Fatih Bilgili, 'İnternet ve Anonim Ortaklık Genel Kurul Toplantısı' (2004) Necip Kocayusufpaşaoğlu İçin Armağan 565, 584.

19 In such cases, shareholders who wish to exercise their indispensable rights arising from shareholding, such as the right to speak and ask questions may be restricted to shareholders having a minimum share capital amount of 100,000 euros or 1% of the share capital, Hopt (n 12) 6. Other conceivable limitations include limiting the number of words or the duration of the videos uploaded to the electronic general meeting system.

transmission of video and audio transmission have been created, and it has been facilitated for people to come together remotely.

Another criticism of virtual general meetings is that they limit the indispensable right of all shareholders to participate in the general meetings by obliging them to participate electronically. The proponents of this view argue that not all shareholders may have the necessary equipment (computer, internet, etc.) to participate in these meetings electronically, and that expecting them to cover these costs would prevent them from attending the general meetings. Similarly, it is claimed that the fact that not all shareholders have the necessary computer and internet usage skills may eliminate the right to participate in the general assembly.²⁰ However, these criticisms are not at a level that requires concern today. Because the use of computers and the internet has become quite widespread and almost everyone has the ability to use them.²¹ Moreover, it is possible to say that these criticisms can be eliminated by the company providing these technical facilities to the shareholders who demand and by providing training on participating in the electronic general assembly system to the shareholders who request it.

3.2. Online general meetings

Unlike virtual general meetings, online general meetings do not take place entirely electronically. In addition to (and simultaneously with) a physical meeting, such meetings offer shareholders the opportunity to participate in the general assembly electronically if they wish. In other words, online general meetings require a physical meeting, but shareholders may also participate in these physical meetings electronically if they demand. For this reason, online general meetings are also referred to as combined model or internet-supported general meetings.²² However, although such meetings provide shareholders with the opportunity to participate electronically, they have not been convenient for the smooth holding of general meetings during the pandemic period, as they require a physical meeting. The general meetings that should have been held during the quarantine periods, especially during the peak of the pandemic, could not be held due to the shareholders' inability to leave their homes. Therefore, it is difficult to characterize online general meetings as an absolute solution that can be applied during extraordinary periods.

20 Stefan Hanloser, 'Proxy-Voting, Remote-Voting und Online HV: § 134III 3 AktG nach dem NaStraG' (2001) *Neue Zeitschrift für Gesellschaftsrecht* 355, 358; This would be contrary to the principle of equal treatment, Bilge (n 13) 225. Also see: Redeke (n 11) 99–100.

21 Redeke (n 11) 100.

22 Bilge (n 13) 225 ff.

4. Situation after COVID-19 outbreak

First of all, the OECD has identified 45 countries that authorized the holding general meetings virtual or hybrid as a consequence of the COVID-19 pandemic.²³ The record attendance at the 2020 and 2021 general shareholders' meetings is a natural consequence of these meetings being held electronically.²⁴ This is in line with the objective of ensuring the desired shareholder democracy by holding general meetings electronically. This high level of participation requires a discussion on whether virtual general meetings can be used more frequently after the pandemic. However, it should be noted immediately that the frequent use of virtual general meetings does not mean making these meetings compulsory. In other words, companies should not be obliged to hold their general meetings virtually, but they should not be prevented from holding these meetings virtually, provided that it is stated in their articles of association. What is meant here can be better understood from the figure²⁵ below:



Figure 1. Source: OECD Publishing (2021 Paris) at <<https://doi.org/10.1787/0fe52016-en>>.

Considering this figure, it is possible to say that there is a tendency towards 'permitted under certain conditions' and 'encouraged' options in the process after the pandemic. Due to the criticisms regarding the electronic general meeting system, it is possible to say that it is more accurate that virtual general meetings should not become 'mandatory'. Indeed, as the title of this study suggests, virtual general meetings should be considered as a lifeguard in extraordinary periods, and it may be more appropriate for companies that can hold their meetings physically to continue these meetings in the classical method for themselves and their shareholders.

It is difficult to predict whether making these meetings mandatory will be more beneficial for the company and shareholders in the long run. However, it is possible to say that holding general meetings virtually in the presence of certain conditions, as in the amendments made in German law in 2022, is the most appropriate procedure in the short term. In German law, virtual general

23 OECD, *The Future of Corporate Governance in Capital Markets Following the COVID-19 Crisis*, Paris, 30 June 2021, 72 table 3.3.

24 Hopt (n 12) 3.

25 Emeline Denis and Daniel Blume, *Using digital technologies to strengthen shareholder participation* [2021] OECD Going Digital Toolkit Notes, No. 9, OECD Publishing, Paris <<https://doi.org/10.1787/0fe52016-en>> accessed on 8 February 2023, 13.

meetings are not mandatory and companies are given freedom to choose the meeting method.²⁶

Since art 118a, which was added to the German Stock Corporation Act in July 2022,²⁷ stipulates strict conditions for virtual general meetings, this regulation may be taken as an example by other countries in the post-pandemic period. According to the first paragraph of this provision, the articles of association may stipulate that the general meetings shall be held virtually or the board of directors may be authorized to do so. In other words, in the first case, the general meetings are held virtually in accordance with the articles of association, while in the second case, the board of directors decides whether or not these meetings should be held virtually. In the absence of a provision on virtual general meetings in the articles of association of the company, it is not possible to hold the general meeting of that company virtually.²⁸ Virtual general meetings can be prescribed for only a limited period of time of no more than five years in accordance with the articles of association.²⁹ When this period expires, it is possible to extend it by adding a new provision to the articles of association.³⁰

According to art 118a of the Stock Corporation Act, after this precondition that virtual general meetings are allowed, there are eight other conditions that must coexist in order for the general meetings to be held virtually. These conditions are as follows:

1. Transmission of the entire meeting by video and audio,
2. Exercise of shareholders' voting rights by means of electronic communication as well as by proxy,
3. Right to submit motions and voting proposals by video communication,
4. Electronic right to information,
5. Making the report of the board of directors or its main contents available no later than seven days before the meeting, but only if the managing board decides that questions of shareholders must be asked electronically before the virtual general meeting.
6. Electronic right to comment,
7. Possibility to speak at the meeting by means of video communication, and
8. Electronic possibility to object to a resolution of the general meet-

26 Stefan Mutter, 'Gekommen um zu bleiben – der Referentenentwurf des Bundesministeriums der Justiz zur Einführung virtueller Hauptversammlungen von Aktiengesellschaften' (2022) *Die Aktiengesellschaft* 57.

27 Stock Corporation Act of 6 September 1965 (Federal Law Gazette I, p. 1089), as last amended by Article 7 of the Act of 22 February 2023 (Federal Law Gazette 2023 I no. 51).

28 Alexander Walch and Stephanie Häuslmeier, 'Die "neue" virtuelle Hauptversammlung' (2023) *Deutsche Notar-Zeitschrift* 106, 109.

29 Art 118a(3) of the Stock Corporation Act.

30 This is intended to give shareholders the chance to terminate the virtual general meetings if the shareholder structure changes or if shareholders no longer wish to hold a virtual general meeting, Walch and Häuslmeier (n 27) 110.

ing.³¹.

As a final remark, it is possible to say that these conditions in German law can be implemented in other countries and the virtual general assembly application may be made permanent in the post-pandemic period.

31 Hopt (n 12) 4.

SECTION 2 – PERSONAL RIGHTS AND FAMILY MATTERS

Circulation of Foreign Public Documents in the Digital Age from a Croatian Legal Perspective^{****}

*Mirela Župan **

Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
ORCID 0000-0002-6673-1274

*Paula Poretti ***

Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
ORCID 0000-0001-6311-8274

*Jura Golub ****

Faculty of Law Osijek, Josip Juraj Strossmayer University of Osijek
ORCID 0000-0002-2440-8081

DOI: 10.54103/milanoup.215.c456

Abstract

This paper examines the legalization of foreign public documents from the perspective of Croatian law. It places particular emphasis on the modern context shaped by the integration of information and communication technologies in civil justice. The proliferation of electronic public documents raises critical issues regarding the applicability of existing norms to the full or partial legalization of such documents and their printouts, whether intended for use in Croatia

**** This paper is based on the research of co-authors: Mirela Župan, Paula Poretti and Jura Golub, 'Strane javne isprave u digitalno doba'in Jakša Barbić (ed), *Međunarodno privatno pravo i globalni trendovi* (Hrvatska akademija znanosti i umjetnosti 2024) (*in press*).

* This paper is a product of work that has been fully supported by the Faculty of Law Osijek Josip Juraj Strossmayer University of Osijek under the project 'Contemporary Issues and Problems of Protecting and Promoting Human Rights'.

** This paper is a product of work that has been fully supported by the Faculty of Law Osijek Josip Juraj Strossmayer University of Osijek under the project 'Contemporary Trends in the Development of Croatian Civil Justice'.

*** The work of doctoral student Jura Golub has been fully supported by the 'Young Researchers' Career Development Project – Training New Doctoral Students' of the Croatian Science Foundation. ORCID: <<https://orcid.org/0000-0002-2440-8081>>

or abroad. From a methodological perspective, this contribution is based on qualitative research within international civil procedural law. It employs standard legal research methods, including doctrinal analysis, formal-logical reasoning, historical analysis, and comparative approaches, focusing on European and selected national legal systems. Regarding the qualification and use of foreign electronic documents as public documents in Croatia, the paper advocates that documents created in electronic form should be regarded as public documents. The *lex loci actus* should determine the status of their printouts, i.e., whether they also qualify as public documents. A contribution of this paper lies in its analysis of the challenges associated with using Croatian electronic public documents abroad. The Republic of Croatia does not issue paper apostilles for electronic public documents signed or certified with a qualified electronic signature or seal. Nor does it issue apostilles for printouts of electronic public documents, as such printouts are deemed mere copies rather than certified duplicates eligible for apostilles. To ensure legal certainty, the paper recommends that individuals intending to use Croatian public documents abroad obtain them in paper form, bearing a handwritten signature and the issuing authority's mechanical seal. Given that an apostille should ideally be physically attached to the document it certifies, the paper underscores the importance of integrating e-Apostilles with electronic public documents. Adding an apostille to a printout of an electronic document undermines the document's digital certification and added value. Furthermore, scanning such printouts results in a non-machine-readable format, a practice not supported by the Hague Conference on Private International Law. The paper concludes by advocating for Croatia's accession to the e-Apostille Program for domestic public documents intended for international use.

Keywords

Apostille Convention, digitalization, e-Apostille, Electronic Public Documents, Foreign Public Documents, International Civil Procedural Law, Legalization

1. Introduction

Public documents are practically used for various purposes in everyday life. Through national regulations, each country regulates the procedure for issuing and the form of individual types of documents. In national legal traffic, there are no significant difficulties regarding the formal validity and authenticity of public documents. Namely, if a public document is issued by the body of the state in which it is used, there are no particularly challenging legal problems. However, if a public document issued by an authorised body of one state needs to be used in another state for the purpose of exercising a right or fulfilling an

obligation, there are a number of legal questions and dilemmas. The number of questions has been increasing in recent times due to the use of information and communication technologies and the digitalisation of national, European, and international civil adjudication.

This paper provides a detailed legal framework for legal traffic of foreign public documents. At the same time, theoretical models of full legalisation, certification by an Apostille, and the exemption from legalisation are delineated. Although each model follows a specific legal path, some doctrinal and practical questions arise in all of them. For example, the question of the conceptual definition and scope of the concept of a public document subject to verification in cross-border legal traffic arises in each of the models.

Therefore, the paper initially examines the conceptual definition of public documents, both domestic and foreign, in Croatian law, and considers their evidentiary value in that regard. National, international, and European legal regimes governing the circulation of public documents in international or cross-border legal traffic is analysed in the third part of the paper, while the provisions of Croatian law in the context of the need for the legalisation of foreign court decisions as public documents in the process of recognising foreign court decisions based on the Private International Law Act (hereinafter referred to as 'the PIL Act') are analysed in the fourth part of the paper. Finally, certain conclusions are offered in the fifth part of the paper regarding the questions raised or discussed in the paper.

2. Public documents in Croatian law

Before providing a substantive definition of public documents in Croatian law, it is necessary to generally define the concept of a document as a higher generic term. According to Triva and Dika, '*a document is any object on which some thought is recorded in writing*', regardless of the medium and means by which the document is written, or the language or type of script used.¹ Within the given definition of a document, it is possible to differentiate types of documents based on a number of criteria. The first criterion for a classification of documents is based on their content, and it is thus possible to distinguish between dispositive (constitutive) and evidentiary documents.² Dispositive documents are considered to be all those documents that contain a legal act (a contract, an offer, termination, a will, etc.), as well as individual acts of state bodies, because they express legally relevant intent.³ To avoid misconceptions, it should be emphasised that in terms of judicial and administrative decisions as proof,

1 Siniša Triva and Mihajlo Dika, *Gradansko parnično procesno pravo* (Narodne novine 2004) 511.

2 Borivoje Poznić, *Gradansko procesno pravo* (Savremena administracija, 1989) 263.

3 *ibid.*

the concept of a constitutive document, which is a synonym for a dispositive document, is by no means limited exclusively to constitutive decisions but it also includes declaratory and condemnation decisions.⁴ The constitutive nature of a document is evident solely in the fact that it contains an expression of legally relevant intent and thereby has the significance of a legal act it embodies.⁵ On the other hand, only those documents whose purpose is to confirm that a specific legal relationship has arisen, regardless of the document itself (eg state registry, land registry, and court register extracts, etc.), are considered evidentiary documents.⁶

In the context of the topic of this contribution, but also generally, the most important classification of documents is the one dividing them into public and non-public (private) documents, which is based on an issuer's authority and the form of such document.⁷ The Civil Procedure Act⁸ (hereinafter referred to as 'the CPA') lays down a general definition of a public document, which is defined as 'a document that has been issued in the prescribed form by a state authority within the limits of its competence, and a document issued in such form by a legal or natural person in the course of executing its public authority, assigned to it by law or a regulation based on the law'.⁹ In this regard, the constitutive elements of a public document are comprised of the authorised body or person as a document issuer, compliance with the prescribed form of the document, and document issuance within the scope of the issuer's jurisdiction or public authority.¹⁰ The lack of any of the aforementioned elements deprives the document of its status of public document, and such a document should be considered a non-public (private) document.¹¹

A similar definition of public documents, albeit somewhat narrower in scope, is also regulated by the General Administrative Procedure Act¹² (hereinafter referred to as 'the GAP Act'). According to the GAP Act, a public document is considered to be a document issued by the competent court or an administrative body within the limits of their competence and in a prescribed form.¹³ The concept of a public document under the GAP Act is narrower in

4 Mihajlo Dika, *Gradansko parnično pravo: Uvrđivanje činjenica* (Narodne novine 2018) 511.

5 *ibid.*

6 Poznić (n 2) 263; Dika (n 4) 511.

7 Dika (n 4) 510.

8 Civil Procedure Act, Official Gazette of the Socialist Federal Republic of Yugoslavia, Nos 4/77, 36/77, 6/80, 36/80, 43/82, 69/82, 58/84, 74/87, 57/89, 20/90, 27/90, 35/91, and Official Gazette, Nos 53/91, 91/92, 58/93, 112/99, 88/01, 117/03, 88/05, 02/07, 84/08, 96/08, 123/08, 57/11, 148/11, 25/13, 89/14, 70/19, 80/22, 114/22, 155/23.

9 CPA, art 230(1).

10 Triva and Dika (n 1) 513.

11 Đuro Vuković, *Međunarodno gradansko procesno pravo* (Informator 1987) 77.

12 General Administrative Procedure Act, Official Gazette, Nos 47/09, 110/21.

13 GAP Act, art 60(2).

scope because it exclusively covers documents issued by competent courts and public authorities (state administration bodies and other state bodies, bodies of local and regional self-government units, and legal entities with public authorities),¹⁴ while documents issued by individuals exercising public authority, such as notaries public, are outside the scope of the aforementioned provision of the GAP Act.¹⁵ In addition to the general definitions of public documents according to the CPA and the GAP Act, specific acts attribute *expressis verbis* the status of public document to certain documents. For example, the Notaries Public Act attributes the status of public document to notarial documents (notarial acts, notarial records, and notarial certificates) and their certified copies, while the Act on Higher Education and Scientific Activity prescribes that diplomas, certificates, and diploma supplements issued by a higher education institution based on public authority are public documents.¹⁶ Furthermore, the State Registries Act stipulates that state registry books, extracts from registry books, and certificates issued based on registry books are also public documents.¹⁷ Certificates of facts that other public authorities maintain official records of are also considered public documents.¹⁸

Furthermore, with respect to the place of issue or the issuer itself, documents can be domestic or foreign.¹⁹ The foreign character of a document is determined according to the *lex fori*, unless otherwise specified by international treaties or legally binding EU acts.²⁰ In this regard, the foreign character of a document, as well as the classification of foreign documents as public documents, will be examined separately in this paper within the framework of specific legal sources, ie from the perspective of autonomous Croatian law, international treaties, and European secondary law.

2.1 Evidentiary value of foreign public documents

The fundamental classification of documents into public and private is important from the perspective of the evidentiary value enjoyed by public documents in legal traffic, thus simplifying the establishment of facts in certain legal protection procedures, thereby also achieving efficiency and effectiveness in proceedings. The evidentiary value of a public document lies in its ability to prove the authenticity of what is confirmed or determined by such a

14 *ibid* art 1.

15 cf CPA, art 230(1) and GAP Act, art 60(2).

16 Notaries Public Act, Official Gazette, Nos 78/93, 29/94, 162/98, 16/07, 75/09, 120/16, 57/22 (hereinafter referred to as: 'the NP Act'), art 3(1)(2); Act on Higher Education and Scientific Activity, Official Gazette, No 119/22, art 73(3).

17 State Registries Act, Official Gazette, Nos 96/93, 76/13, 98/19, 133/22 (hereinafter referred to as 'the SR Act'), art 2(2).

18 GAP Act, art 159(1)(2).

19 Triva and Dika (n 1) 513.

20 Vuković (n 11) 77.

document.²¹ It is about a rebuttable presumption of authenticity of a public document, which is based on the maxim *acta probant sese ipsa*, recognised by most legal systems within the continental legal system.²² Two further presumptions are derived from the general presumption of authenticity of public documents, ie that in terms of authenticity, a document emanates from the body indicated on the document as the issuer, and that the content of the document established within the issuer's jurisdiction is authentic.²³ These presumptions, as well as the evidentiary value of a public document itself, together with such a status granted on the basis of regulations, derive their specific evidentiary value from the public authority of the document issuer and the procedure preceding the issue of the public document, ie that the issuer issued the document within its jurisdiction.²⁴ These are constitutive elements from which the specific status of public document is drawn, which originate in Roman law and have essentially remained unchanged to this day.²⁵ Therefore, within the evidentiary proceeding of a specific lawsuit in which a particular public document was used, a party that disputes the authenticity of a public document can submit counter-evidence to rebut the presumption of authenticity of the public document.²⁶ Moreover, it is possible to initiate a separate lawsuit by an action for a declaratory judgment, the main issue of which will be to determine whether the document is authentic or fake.²⁷ In this regard, it should be emphasised that the given formal rule of evidence referring to the presumption of authenticity of public documents is an exception to the principle of free evaluation of evidence, because the law prescribes the evidentiary value of such documents.²⁸ However, this presumption does not apply in all protective legal proceedings. In this context, an exception is a criminal procedure in which the presumption of authenticity of public documents does not apply, hence in terms of the evidentiary value, public documents are equated with private documents.²⁹ Due to their importance in legal traffic, or the presumption of authenticity, public documents also receive

21 Poznić (n 2) 265.

22 Christian Hertel, 'Legalization of public documents' in Jürgen Basedow and others (eds), *Encyclopedia of Private International Law* (Edward Elgar Publishing, 2017) 1094–1095.

23 Triva and Dika (n 1) 514.

24 European Law Institute, International Institute for the Unification of Private Law, *ELI - UNIDROIT Model European Rules of Civil Procedure* (OUP 2021) 159.

25 Ivan Milotić, 'Pravno uređenje položaja sastavljača isprava te povjerenja u privatne isprave u rimskom pravu' in Alan Uzelac and others (eds), *Djelotvorna pravna zaštita u pravičnom postupku - Izazovi pravosudnih transformacija na jugu Europe* (Pravni fakultet Sveučilišta u Zagrebu 2013) 721.

26 CPA, art 230(3).

27 *ibid* art 187(1).

28 Triva and Dika (n 1) 511.

29 Davor Krapac, *Kazneno procesno pravo, Prva knjiga: Institucije* (7th edn, Narodne novine 2015) 508.

special protection at the criminal law level through the qualified form of the criminal offense of document forgery.³⁰

Since the question of the evidentiary value falls within the realm of procedural law, the evidentiary value of a foreign public document will generally always be assessed in the receiving country according to the *lex fori*, which ultimately can also result in the foreign public document not enjoying the same strength in the issuing country and the receiving country.³¹ Therefore, comparatively speaking, there are examples where the evidentiary value of a foreign public document is assessed according to the *lex loci actus*.³² The relevance of the *lex fori* is also accepted by Croatian civil procedural law, and it is thus prescribed that foreign public documents enjoy the same evidentiary value as domestic public documents, under the condition of reciprocity and provided that they are duly certified, unless otherwise specified by an international treaty.³³ From this, it follows that the Croatian legislator has opted for a stricter approach in this regard, pursuant to which, under cogent assumptions, foreign public documents can enjoy the same evidentiary value as domestic public documents. From a comparative perspective, German civil procedural law is considerably more flexible in this regard. A German court is authorised by discretionary judgment to assess whether a foreign public document is authentic or true, without the need for specific additional evidence, such as certification, to support the authenticity of the foreign public document.³⁴ However, in cases where the court exercises discretion to deny the authenticity of the foreign public document, this can be remedied by legalisation of a foreign public document by the German consul or federal minister.³⁵

Following all of the above, in order to achieve equivalence in the evidentiary value of foreign public documents with domestic public documents, three legal regimes are differentiated with respect to the country issuing the foreign public document. The first category encompasses certain categories of public documents originating from EU Member States, which fall within the scope of application of EU secondary law; the second category of foreign public documents consists of documents originating from countries with which the Republic of Croatia has concluded binding bilateral or multilateral treaties that define the legal status of public documents between the contracting states; and finally, the third category of foreign public documents includes all those documents whose

30 Criminal Code, Official Gazette, Nos 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, art 278.

31 Hertel (n 22) 1103.

32 Vuković (n 11) 79.

33 CPA, art 231.

34 Code of Civil Procedure (Zivilprozessordnung) (Germany) <https://www.gesetze-im-internet.de/englisch_zpo/index.html> accessed on 14 January 2024 (hereinafter referred to as 'ZPO'), §438(1).

35 *ibid* § 438(2).

status is not defined in accordance with the aforementioned legal regimes, and in such cases, their legal status is governed solely by autonomous Croatian law.³⁶

3. Fundamental considerations of the circulation of foreign public documents

The issue of foreign document verification is not of recent origin; on the contrary, it has been a challenge for cross-border legal traffic for decades. The basic model of legalisation, ie legalisation of documents for their use abroad, is today just one of the legal ways, but also the most complex one, of using foreign public documents. Namely, models of cooperation between states are being developed that are aimed at faster, simpler, and more secure use of public documents abroad. In addition to national rules on the legalisation of foreign documents, several additional tracks have been developed for the circulation of foreign documents. In principle, we distinguish four groups of legal sources dealing with the issue of the circulation of foreign public documents, depending on whether they are based on national regulations, multilateral cooperation, bilateral cooperation, or European Union common law. Within these four groups, we can also distinguish several different models by which the circulation of foreign public documents is carried out. What poses an equally big challenge for each of these possible paths is digitalisation, which is discussed within each of the following chapters.

3.1 Full legalisation

Cross-border legal traffic also includes the use of foreign public documents. Lawyers encountered this problem as early as the 17th century, within the framework of the then legal traffic. They sought legal solutions with great caution, partly because of their lack of knowledge of foreign legal systems and related documents, and partly because of fear of possible falsification of documents or other illegal actions. Then the model was introduced aimed at verifying document authenticity through its legalisation, which precedes its use on the territory of another country. The document authentication method is based on a certification made by a consular agent of the country in the territory of the country of origin of the document. Consular authentication or legalisation is the authentication of a document by a diplomatic or consular agent of the country receiving the public document, who is at the time of authentication in the country issuing the document.³⁷ Namely, it is considered that the diplomatic mission or consulate of the country receiving the document, which is located in the country issuing the public document, has more detailed information

36 Dika (n 4) 536–537.

37 Hertel (n 22) 1098.

about the competent authorities of the issuing country, as well as the prescribed procedures for issuing the document.³⁸ Since the middle of the 19th century, most countries have opted for an authentication chain. This model is based on a series of certifications that follow one after another,³⁹ whereby the one that follows in the certification process can verify with certainty the identity of the previous signer or seal. The last certification in the series is granted by the consulate, which certifies legalisation of the document with its authentication.⁴⁰

With respect to the implementation of the foreign public document legalisation procedure, autonomous Croatian law, as a separate legal regime, includes all public documents whose status is not defined in accordance with legally binding EU acts, ie binding bilateral or multilateral international treaties.⁴¹ The autonomous Croatian legal source, which regulates the matter in question, is the Act on the Legalisation of Public Documents in International Legal Traffic⁴² (hereinafter referred to as 'the LPD Act'). First of all, it is necessary to determine when a certain document is considered a foreign document from the aspect of Croatian law, ie when there is an element of foreignness in relation to an individual foreign document. In this sense, the LPD Act is committed to the territoriality principle, meaning that a foreign public document is considered to be a document 'issued abroad'.⁴³ Therefore, *Dika* justifiably objects that the place of drafting the document should not be relevant, and argues that the criterion of legal order on the basis of which a certain state body or other person acquired public powers should be taken as relevant, since the bodies of one state, for example diplomatic missions and consulates, can draw up public documents on the territory of another country.⁴⁴

In terms of the qualification of a certain foreign document as a public document, the LPD Act considers a public document to be a document that is considered a public document in the country in which it was issued and that was issued in the form and manner prescribed by the law of that country.⁴⁵ Or simply put, the law applicable to the qualification of a foreign document as a public document is the *lex loci actus*.⁴⁶ In this regard, from the perspective of the

38 *ibid.*

39 *The International Legalization Handbook* (Chancellor Publications 1996) 7.

40 Peter Zablud, 'The 1991 Apostille Convention – authenticating documents for international use' in Thomas John, Rishi Gulati, Ben Kohler (eds), *The Elgar Companion to the Hague Conference on Private International Law* (Edward Elgar Publishing 2020) 278-279.

41 LPD Act, art 1.

42 Act on the Legalisation of Public Documents in International Legal Traffic, Official Gazette, Nos 06/73, 53/91.

43 *ibid* art 3(1).

44 *Dika* (n 4) 516.

45 LPD Act, art 3(3).

46 Đuro Vuković and Eduard Kunštek, *Međunarodno građansko postupovno pravo* (Zgombić & Partneri 2005) 201.

Croatian authorities that may be presented with a foreign document, the question arises of the possibility of determining the content of the law of the issuing country on whether a specific document is considered a public document pursuant to the law of that country. Given that the LPD Act does not provide for the method of determining the content of the law of the country issuing the document, the rules of the Private International Law Act⁴⁷ (hereinafter referred to as ‘the PIL Act’) on determining the content of the law of a foreign state should be applied in the aforementioned case. Namely, the court, as well as other bodies of the Republic of Croatia, is obliged to determine the content of the law of a foreign state *ex officio*, and the maxim *iura novit curia* is applied with regard to foreign law.⁴⁸ However, given the possible difficulties in determining the content of foreign law, the PIL Act makes a kind of exception to the general rule according to which the content of abstract legal norms cannot be the subject of proof.⁴⁹ Thus, the court is authorised to request notification of the content of foreign law from the ministry responsible for judicial affairs or any other body, as well as from experts or specialised institutions, but the parties themselves are also authorised to submit public and private documents to the court about the content of foreign law.⁵⁰ The possibility of the parties to submit documents on the content of foreign law is their authority, but not their duty. Therefore, the parties cannot bear the negative consequences of not submitting a document on the content of foreign law. This is because the determination of the content of foreign law is a legal, not a factual issue, hence the burden to prove the content of foreign law does not lie with the parties, nor can the maxim *da mihi factum, dabo tibi ius* be applied.⁵¹ However, it should be borne in mind that the procedure for determining the content of foreign law can sometimes take an unreasonably long time, especially in relation to the content of the law of countries with which the Republic of Croatia does not maintain frequent legal traffic and diplomatic relations are not significantly developed. Therefore, it would not be opportune to ultimately persist in determining the content of foreign law if it would significantly affect the duration of the entire legal protection procedure with a legal question of the public character of a foreign document. This is because lengthy procedures for determining the content of foreign law could represent a violation of the right to a trial within a reasonable time as a component of the right to a fair trial guaranteed by the Convention

47 Private International Law Act, Official Gazette, Nos 101/17, 67/23.

48 Mirela Župan, ‘The New Croatian Private International Law Act – Something Old, Something New and much Borrowed’ [2020/2021] Yearbook of Private International Law 388; PIL Act, art 8(1).

49 Triva and Dika (n 1) 183.

50 PIL Act, art 8(3)(4).

51 Triva and Dika (n 1) 184.

for the Protection of Human Rights and Fundamental Freedoms.⁵² In that case, if determining the content of foreign law took an unreasonably long time, but also if the *lex loci actus* could not be applied for any reason, the *lex fori* would exceptionally be applicable to determining the public character of a foreign document, ie from the point of view of national implementation bodies - the Croatian law.⁵³

In terms of the LPD Act, legalisation or certification of the document verifies the authenticity of the signature of the person who signed the document and the authenticity of the seal printed on the document.⁵⁴ A *stricto sensu* interpretation of LPD Act leads to the conclusion that legalisation does not verify the capacity of the person who signed a public document. However, there is an opinion that by legalising the signature of the person who signed the document, the capacity in which a certain person signed a certain public document is also confirmed (a judge, a notary public, a court official, a state administration body official, a dean, a director, etc.).⁵⁵ This understanding is not without support. Namely, the mere verification of a person's signature, without confirming the capacity of the signer, does not yield the desired legalisation effects, ie it does not provide evidence that a certain person at a certain time when the public document was drawn up really acted in a certain capacity, which plays a decisive role in assessing both the very nature and the content of the document that is to be legalised. Comparatively speaking, it is possible to differentiate between legalisation in the narrower sense, which includes only the verification of the authenticity of a signature, the signer's capacity and the seal on the public document, and legalisation in the broader sense, which includes everything encompassed by legalisation in the narrower sense, plus confirmation that the public document issuer acted within its jurisdiction and that the procedure for issuing the document in question was carried out pursuant to the law of the country of origin of the document.⁵⁶ Autonomous German consular law, which governs the legalisation procedure of foreign public documents, recognises both previously explained types of legalisations.⁵⁷ Namely, upon request, and provided that there is no doubt about the legal situation, a German consul is authorised to confirm in a note on the document that the document issuer was authorised to issue the document and that the document was drawn up in accordance with

52 Župan (n 48) 389; the Convention for the Protection of Human Rights and Fundamental Freedoms, Official Gazette - International Treaties, Nos 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, 13/17, art 6(1).

53 Vuković and Kunštek (n 46) 201; PIL Act, art 8(5).

54 LPD Act, art 3.

55 Dika (n 4) 538.

56 Hertel (n 22) 1095.

57 Consular Act (Konsulargesetz) (Germany) <<https://www.gesetze-im-internet.de/konsng/>> accessed on 14 January 2024, §13.

the law of the document's place of issue.⁵⁸ On the other hand, autonomous Croatian law has exclusively applied legalisation in the narrower sense.⁵⁹

The public document legalisation process consists, as a rule, of two stages, ie the process of internal and international legalisation, whereby the implementation of one or both processes depends on the national laws of the country issuing the document and the country receiving the document.⁶⁰ From the perspective of Croatian public documents, which are intended to be used abroad, depending on the law of the country receiving the Croatian public document, it is possible that it will be necessary to carry out an internal legalisation procedure before the Croatian authorities.⁶¹ Accordingly, in the first step, the judge or municipal court president certifies the signature and seal of the public document issuer, after which there follows the legalisation procedure, which consists in the Ministry of Justice and Administration legalising the seal and signature of the judge or court president, and only then, in the third step, the Ministry of Foreign and European Affairs or the diplomatic and consular representations of the Republic of Croatia certify a public document intended for use abroad.⁶² However, in order for the public document thus ultimately certified by the Croatian Ministry of Foreign and European Affairs or the diplomatic and consular representations to be used abroad, it is possible that it will be necessary to carry out an additional procedure of international legalisation of the Croatian public document, which is carried out before the state authorities in which the Croatian public document is to be used. In the opposite situation, when a foreign public document is to be used before the authorities of the Republic of Croatia, then the Croatian Ministry of Foreign and European Affairs or a diplomatic and consular representation abroad carries out the international legalisation procedure, ie they confirm the authenticity of the signature and seal on the foreign public document.⁶³

Internal legalisation of Croatian public documents, which is carried out by municipal courts, does not fall within the scope of any specific legal protection procedure, such as a non-contentious procedure, but certification of documents intended for use abroad is covered by court administration.⁶⁴ This applies equally to the addition of an Apostille based on the Apostille Convention, as well as the implementation of the internal legalisation procedure based on the LPD Act.

58 *ibid* § 13(4).

59 LPD Act, art 2.

60 Vuković and Kunštek (n 46) 203–204.

61 Vuković and Kunštek (n 46) 203–204; LPD Act, art 5.

62 LPD Act, arts 6 and 7(1).

63 *ibid* arts 2 and 3(1).

64 Judiciary Act, Official Gazette, Nos 28/13, 33/15, 82/15, 82/16, 67/18, 126/19, 130/20, 21/22, 60/22, 16/23, art 29(1).

With regard to the use of digital public documents, which originally exist exclusively in electronic form, it should be considered that, regardless of a qualified electronic signature/seal, they fall within the scope of the LPD Act and should be properly legalised in accordance with that act when the Republic of Croatia is the document receiving country. Namely, the LPD Act imperatively stipulates that foreign public documents can be used in the Republic of Croatia only if they are certified by the Ministry of Foreign and European Affairs or a diplomatic and consular representation of the Republic of Croatia abroad. Accordingly, in addition to the aforementioned international legalisation of electronic public documents when the Republic of Croatia is the document receiving country, it would be appropriate to certify Croatian electronic public documents through internal legalisation when they are intended for use abroad. This is because the purpose of legalisation is, *inter alia*, to confirm the capacity of the signer of a certain public document, ie that a certain person really acted in the capacity indicated on the document at the time of drawing up that public document.⁶⁵ The sole purpose of the provisions on the recognition of qualified electronic signatures in electronic legal traffic is to recognise the equivalence between handwritten signatures and qualified signatures by legal effect, while data integrity and the accuracy of data sources with which the qualified electronic seal is associated are assumed for qualified electronic seals.⁶⁶ Special attention should also be paid to public documents that originally existed in electronic form, but were subsequently printed on paper. Namely, in each individual case, whether a document written in this way still has a public character will depend on the *lex loci actus*, because the aforementioned rule refers to the law of the country where the document was drawn up, even in terms of the form of a document.⁶⁷ From the aspect of Croatian public documents, electronic records generated from the official records of public sector bodies have the status of public documents, and they have that status even when they are printed on paper, provided that the documents (records) printed in this way contain data for verifying the credibility of the electronic record via a website.⁶⁸ However, it should be emphasised that electronic records printed in this way, eg public documents obtained through the e-Citizens system, have a limited legal life. Namely, after the expiration of a three-month period, the generated electronic record for verification is deleted from the system, and it is no longer possible to check the authenticity of the printed electronic record. Consequently, an

⁶⁵ See n 55.

⁶⁶ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257, arts 25(2) and 35(2).

⁶⁷ LPD Act, art 3(3).

⁶⁸ Regulation on Organisational and Technical Standards for Connecting to the National Information Infrastructure, Official Gazette, No 60/17, art 15(1)–(3).

electronic record printed on paper loses its status as a public document, ie it is no longer legally valid.⁶⁹

For comparison purposes, on the basis of autonomous Slovenian law, the Republic of Slovenia also subjects public documents drawn up in electronic form to legalisation. For this purpose, Slovenian state bodies and other public authority entities are obliged to notify the competent court, for the purpose of judicial certification in the internal legalisation process, *inter alia*, of electronic signature certificates with which their employees electronically sign public documents issued in electronic form in order to verify the authenticity of the electronic signature on the original electronic public document during the authentication procedure.⁷⁰ Notaries public are obliged to notify the ministry responsible for justice of the electronic signature certificates.⁷¹

3.2 Bilateral regimes

By taking over previous bilateral treaties on legal assistance by succession or by concluding new treaties after 1991, the Republic of Croatia has continued to facilitate the circulation of public documents. Thus, bilateral regimes regulating this issue can be found in treaties concluded with many countries in the wider region, ie Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Montenegro, the Czech Republic, France, Greece, Italy, Hungary, North Macedonia, Poland, Romania, Slovenia, Slovakia, Serbia, the Russian Federation, and Turkey.⁷² As a rule, full exemption from legalisation is defined with reference to the types of documents. For example, in relation to the Kingdom of Belgium, there are two bilateral treaties in force, one regulating the circulation of public documents originating from courts,⁷³ and the other from registry offices.⁷⁴ Documents not

69 *ibid*, art 15(1)–(4).

70 Act on the Authentication of Documents in International Legal Traffic, Official Gazette of the Republic of Slovenia, No 9/17, arts 4(1) and 6(4).

71 *ibid*, art 4(2).

72 See the Ministry of Foreign and European Affairs of the Republic of Croatia, 'Overview of Bilateral International Treaties of the Republic of Croatia by Country' <<https://mvep.gov.hr/vanjska-politika/bilateralni-odnosi/pregled-dvostranih-medjunarodnih-ugovora-republike-hrvatske-po-drzavama/21905>> accessed 10 January 2024.

73 'In order for documents or instruments drafted, issued, or authenticated by the courts of one of two states to be utilized in judicial proceedings within the territory of the other state, it is not necessary to legalize them or subject them to any similar formality if they are authenticated by the court seal. This also applies to documents or instruments signed by an authorized court official, if their signature suffices under the law of the state to which the court belongs'; Agreement on Legal Cooperation in Civil and Commercial Matters (Socialist Federal Republic of Yugoslavia–Kingdom of Belgium) (24 September 1971), Official Gazette of the Socialist Federal Republic of Yugoslavia - Annex, No 7/74, art 10.

74 Convention on the Issuance of Extracts from Civil Status Registers and Exemption from Legalisation, (Socialist Federal Republic of Yugoslavia–Kingdom of Belgium) (24 September 1971), Official Gazette of the Socialist Federal Republic of Yugoslavia, No 55/72.

covered by these treaties are subject to the Hague Apostille Convention or the Regulation on Public Documents. This issue is regulated somewhat differently in the treaty concluded with Italy, which, through its arts 19 and 20, actually covers all certified copies of civil status documents, certified copies of decisions, orders, judgments, rulings, and other legal documents, written statements and court documents registered or deposited with these bodies, notarial acts, as well as transcripts and translations of these documents.⁷⁵ An even narrower exemption from legalisation applies to the regime with Slovakia. Here, exemption from legalisation applies only to documents issued by judicial authorities dealing with civil, family, and criminal matters. Documents outside of this scope are subject to other regimes, typically the Hague Apostille Convention or the Regulation on Public Documents.⁷⁶ The circulation of public documents between states through bilateral treaties occurs commonly because this generally eliminates all obstacles in the mutual circulation of public documents.⁷⁷ In addition to the issue of legalisation of public documents, some bilateral treaties go a step further and directly stipulate that documents considered public documents in one contracting state have the evidentiary value as public documents in the territory of the other contracting state.⁷⁸

As to electronic public documents, it should be noted that in the context of a bilateral treaty between contracting states, these documents could be used before the authorities of the other contracting state provided that the *lex fori* recognises such documents. On the other hand, when it comes to the printouts of electronic public documents and the use of such printed documents, consideration should be given to the *lex loci actus*, ie whether the printed electronic document continues to be considered a public document according to the law of the issuing country. All of this, of course, applies if the subject matter is not otherwise regulated by international treaties.

75 Convention on Mutual Legal Assistance in Civil and Administrative Matters (Federal People's Republic of Yugoslavia–Italian Republic) (3 December 1960), Official Gazette of the Federal People's Republic of Yugoslavia - Annex, No 5/63.

76 Treaty Regulating Legal Relations in Civil, Family and Criminal Matter (Socialist Federal Republic of Yugoslavia–Czechoslovakia) (20 January 1964), Official Gazette of the Socialist Federal Republic of Yugoslavia - Annex - International Treaties and Other Agreements, No 13/64; Official Gazette - International Treaties, No 11/97. By Note of 29 April 2013, reference number 25336/2013/81-40620, the application of art 15 of the Treaty has been narrowed.

77 Jonathan Fitchen, 'Authentic Instruments and European Private International Law in Civil and Commercial Matters: Is Now the Time to Break New Ground?' (2011) 7(1) Journal of Private International Law 33, 50.

78 Agreement on Legal Assistance in Civil, Family and Criminal Matters (Yugoslavia–USSR) (24 February 1962), Official Gazette of the Socialist Federal Republic of Yugoslavia - International Treaties and Other Agreements, No 5/63, art 15(2).

3.3 Multilateral regime of the Hague Convention on the elimination of the requirement of legalisation for foreign public documents of 5 October 1961

Multilateral regimes of exemption from legalisation were characteristic of the early activities of the Hague Conference on Private International Law (hereinafter referred to as ‘the HCCH’ or ‘the Hague Conference’) and the International Commission on Civil Status.⁷⁹ The need for exemption from legalisation is also foreseen in some other multilateral international treaties, such as the Convention Providing a Uniform Law on the Form of an International Will of 1973.⁸⁰ In the mid-20th century, the international community became aware that the lengthy and complex process of full legalisation was hindering cross-border legal traffic. The first step in simplifying full legalisation was taken with the Convention on Civil Procedure of 1954, adopted within the framework of the Hague Conference, which stipulated that the documents necessary for marriage can be legalised only by the diplomatic or consular agents of the contracting state.⁸¹ Furthermore, a more specific move to simplify legalisation was made in the following year, ie 1955, when a multilateral treaty was proposed within the Council of Europe that would achieve the same effects with more certain and simpler legalisation procedures.⁸² The Apostille Convention was adopted on 5 October 1961, and it came into effect on 21 January 1965. Together with other conventions adopted from the 1950s to the 1980s, the Apostille Convention forms the backbone of modern Hague conventions that simplify international judicial cooperation, and enable the fourth dimension of private international law.⁸³ The Convention has been applied in the Republic of Croatia since 1991, based on the notification of succession.⁸⁴ Today, more

79 In particular Convention No 17 on the exemption from legalization of certain records and documents, Athens, 15 September 1977. The Republic of Croatia is not a contracting party to the Convention.

80 Convention Providing a Uniform Law on the Form of an International Will, with an annex, Official Gazette of the Socialist Federal Republic of Yugoslavia - International Treaties, No 3/77, art VI. The signature of the testator, of the authorized person, and of the witnesses to an international will, whether on the will or on the certificate, shall be exempt from any legalization or like formality. Nonetheless, the competent authorities of any Contracting Party may, if necessary, satisfy themselves as to the authenticity of the signature of the authorized person.

81 Convention on Civil Procedure, Official Gazette of the Federal People's Republic of Yugoslavia - International Treaties and Other Agreements, No 6/62, and Official Gazette - International Treaties, No 4/94, art 25.

82 The International Legalization Handbook (n 39) 9.

83 Lukas Rass-Masson, ‘The HCCH and legal co-operation – shaping the fourth dimension of private international law’ in Thomas John and others (eds), *The Elgar Companion to the Hague Conference on Private International Law* (Edward Elgar Publishing 2020) 150.

84 Decision on the Publication of Multilateral International Treaties to which the Republic of Croatia is a Party based on Notifications of Succession, Official Gazette - International

than 60 years after its adoption, the Convention has 126 contracting states, with their number increasing year by year.⁸⁵ The Convention consists of a total of 15 articles and one annex.

The structure of the Apostille Convention is traditional, with its first provision defining the substantive scope of application and the concept of 'public document'. The Apostille Convention opts for the territoriality principle, meaning that a foreign document is considered to be only the document drawn up within the territorial jurisdiction of one contracting state and used within the territorial jurisdiction of another contracting state, while documents issued by diplomatic or consular agents of contracting states are excluded from the scope of the Convention.⁸⁶ The territorial scope of application between contracting states means that an Apostille is neither issued nor recognised in legal traffic with non-contracting states or among contracting states that have made the reservation, and in national legal traffic.⁸⁷

New contracting states may accede to the Apostille Convention; however, their accession will have effect only regarding the relations between the acceding state and contracting states that have not raised an objection to its accession within six months after the receipt of the notification. The Republic of Croatia has not made any reservations regarding new accessions, nor has any other contracting state done so with respect to us.⁸⁸

In terms of its relation with other legal sources, the Apostille Convention gives preference to other regimes of exemption from legalisation between contracting states if such regimes are in force.⁸⁹ Therefore, contracting states will not be obliged to apply the Apostille Convention if the document has been abolished or simplified, or if such document has been exempted from legalisation by the autonomous law of the document receiving country or by a treaty between the contracting states. Additionally, the Convention between contracting

Treaties, No 4/94.

85 Convention Abolishing the Requirement of Legalisation for Foreign Public Documents (concluded 5 October 1961), Official Gazette - International Treaties, Nos 4/94, 11/11; Full list of contracting parties available at HCCH, 'Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents - Status table' (2024) <<https://www.hcch.net/en/instruments/conventions/status-table/?cid=41>> accessed 18 January 2024.

86 Apostille Convention, art 1.

87 *Apostille Handbook: Practical Handbook on the Operation of the Apostille Convention* (The Hague Conference on Private International Law - Permanent Bureau 2023) 45 (hereinafter 'Apostille Handbook').

88 For reservations see HCCH, 'Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents - Status table' (2024) <<https://www.hcch.net/en/instruments/conventions/status-table/?cid=41>> accessed 18 January 2024.

89 Jonathan Fitchen, *The Private International Law of Authentic Instruments* (Hart Publishing 2020) 94.

states overrides all treaties whose formalities are more rigorous with respect to the addition of an Apostille in the sense of the Convention.⁹⁰

The Apostille Convention was adopted with the aim of simplifying the circulation of public documents and is based on the mutual recognition of public documents issued by the contracting states.⁹¹ The Convention abolishes the traditional model of legalising foreign public documents and substitutes it with a single certification ('Apostille') issued by the competent authority of the state in which the document was originally issued.⁹² The Convention defines legalisation as a formality by which diplomatic or consular agents of the contracting state in which the document is to be presented certify the authenticity of the signature, the capacity in which the person signing the document acted and, where appropriate, the identity of the seal or stamp which it bears (art 2). By issuing the Apostille certificate, the competent authority certifies the authenticity of the signature on the public document, the capacity in which the person signing the document acted, and the identity of the seal or stamp which the document bears. The Apostille certificate does not guarantee the accuracy of the content of the public document, it does not confirm that all national requirements have been fulfilled for the proper issuance of the public document, nor does it affect the acceptance, admissibility, or evidentiary value of public documents.⁹³

Some contracting states exempt from legalisation the documents to which the Convention applies and that need to be presented within their territory. The only formality that may be required is the addition of an Apostille issued by the competent authority of the state in which the document was issued (art 3(1)). An Apostille is a certificate placed directly on the document itself or attached to the public document, following the model annexed to the Convention. The Apostille can be drawn up in English, French, or the official language of the issuing authority, and the use of multilingual forms is encouraged.⁹⁴

The procedure for issuing the certificate is regulated by arts 5-7 of the Convention. The certificate is issued at the request of the person who has signed the document or of any bearer of the document. In practice, contracting states use several models for submitting requests, including in person, by mail, or by e-mail.⁹⁵ Contracting states may develop a standard request form for this purpose. In a 2003 resolution, the Special Commission stated that failure to strictly adhere to the specific form of the Apostille alone cannot be grounds for rejecting a document. It is mentioned that the Apostille issued by the

90 Apostille Convention, art 8.

91 Gajanan S. Phunde and Sachin S. Tarate, *Lectures on the Law of Evidence* (Rudra Publications 2020) 97–98.

92 Apostille Handbook (n 87) 27.

93 *ibid* 31.

94 *ibid* 75.

95 *ibid* 38.

competent authority should follow as closely as possible the model annexed to the Convention. However, variations in size and shape of the Apostille, which occur among different contracting states whose competent authorities issue the certificate, should not be valid grounds for rejecting an Apostille as long as the Apostille can be clearly identified as the one issued under the Convention.⁹⁶

States themselves develop internal procedures applied by competent authorities when issuing Apostilles. The authorities may introduce mechanisms to reliably verify the authenticity of public documents that need to be certified. Competent authorities usually have a database of seals or stamps and verify the authenticity by comparison. This process is changing due to the increasing use of ICT, making the visual comparison less important as signatures and seals or stamps can be authenticated electronically and often automatically. In this regard, for states that exclusively use electronic public documents, it is no longer necessary to maintain a database because a digital signature carries a certificate which confirms the origin and authenticity of the signer. A digital signature can be easily and reliably verified with the certificate that accompanies it; however, competent authorities will still need to verify whether the authority or person has the capacity to issue that type of public document. In general, this will be verified by scanning the QR code. Therefore, the Permanent Bureau recommends to contracting states digital certificates accredited to an institution or organisation, rather than a person in charge.⁹⁷ If the authenticity cannot be established, the competent authority issuing the Apostille may make additional efforts to verify it, and ultimately, the Apostille may not be issued. A 2009 resolution by the Special Commission stipulates that the Apostille may not be refused in a state in which it is to be used solely on the grounds that it does not comply with all the formalities required for its issuance in that state. Such actions would be considered a double standard.⁹⁸

Depending on whether a public document is in paper (physical) or electronic form, there are several models for its certification. Traditionally, a paper Apostille was accompanied by a paper public document. More recently, in systems that have fully digitalised their justice systems, an e-document is certified with an e-Apostille. However, in partially digitalised systems, there are certain dilemmas regarding the certification of electronic documents, specifically the Apostille certifying them. Since the Apostille should ideally be physically attached to the public document it certifies, an optimal solution would be to link

96 Special Commission Conclusions and Recommendations, 'The Practical Operation of the Hague Apostille, Evidence and Service Conventions' (28 October - 4 November 2003) 5 <http://www.hcch.net/uploadwop/lseconcl_e.pdf> accessed 18 January 2024.

97 Apostille Handbook (n 87) 69–73.

98 Special Commission Conclusions and Recommendations, 'The Practical Operation of the Hague Apostille, Service and Access to Justice Conventions' (2–12 February 2009) 14 <<https://www.hcch.net/>> accessed 18 January 2024.

e-documents to an e-Apostille. In contracting states that have not introduced an e-Apostille system, including the Republic of Croatia, it is common practice to print electronic public documents on paper and then certify them with an Apostille. In this way, specific elements of the certificate of that document are lost. The Hague Conference encourages all states that issue electronic public documents in national legal traffic to adopt the e-Apostille system instead of the current practice.⁹⁹

If a public document exists in paper form, and the contracting state has fully transitioned to an e-Apostille system, the usual procedure would be to scan the paper public document and convert it into an electronic format. The competent authority would then issue an e-Apostille for this electronic document. This process is valid provided that pursuant to the law of that state, the scanned copy has the same legal power as the original. Since such a scanned copy does not have a certificate attached to the signature or seal or stamp, the competent authority must verify the authenticity of the signature or seal or stamp in a traditional way, typically by comparison.

The annex to the Convention contains a model Apostille certificate with ten integral parts. The Apostille includes the following informational items: 1) the document issuing country, 2) the person that signed the underlying document, 3) the capacity in which the person signing the document acted, 4) the identity of the seal or stamp which the document bears, and in relation to the certificate: 5) the place, 6) the date, 7) the person issuing the certificate, 8) the serial number, 9) the seal or stamp, and 10) the signature of the person issuing the certificate. The purpose of this model Apostille is to ensure comparability among other contracting states. No authority should reject an Apostille issued with additional text outside the designated area.¹⁰⁰

The competent authority will refuse to issue an Apostille in the following situations: when the public document is intended for legal use in a non-contracting state, when it is a public document excluded from the scope of the Convention according to art 1(3), when the document is not considered a public document by the country of origin, if the competent authority is not authorised to certify a particular type of document, or if the competent authority has failed to verify the origin of the public document for which the Apostille is requested. The competent authority will issue an Apostille if it is convinced of the authenticity of the public document. It will then record it in a register, which can be either a traditional paper or electronic register for internal use, or an e-register. An e-register is a publicly accessible database, allowing parties to

⁹⁹ Apostille Handbook (n 87) 73.

¹⁰⁰ Special Commission Conclusions and Recommendations, 'The Practical Operation of the Hague Apostille, Service and Access to Justice Conventions' (2 - 12 February 2009) 14 <<https://www.hcch.net/>> accessed 18 January 2024.

verify issued Apostilles. Contracting states can enter both paper Apostilles and e-Apostilles into the e-register.¹⁰¹

The authorities responsible for issuing Apostilles are determined by each contracting state,¹⁰² and they must notify the Ministry of Foreign Affairs of the Netherlands of these authorities or of any changes thereto. The three fundamental functions of these national authorities are as follows: to verify the authenticity (origin) of the public document, to issue the Apostille, and to maintain a register of the issued Apostilles.¹⁰³ It is recommended that certification be carried out in a single procedure, exclusively before the competent authority.¹⁰⁴ However, some states have introduced additional formalities and a multi-step process for issuing Apostilles.

Since the purpose of this system is to enable the use of foreign public documents within the territory of other contracting states, by becoming a party to the Convention, each state has committed to giving legal effect to certified documents from other contracting states. However, the receiving country may still refuse to accept the Apostille if it was issued by a non-contracting state, if the document to which the Apostille is attached is not considered a public document in the country of origin, if the Apostille was issued by the authority not competent to issue an Apostille or by a competent authority outside the scope of jurisdiction, if the Apostille does not contain the ten essential informational items, if it is not attached to the public document it certifies, or if it is a forged or subsequently altered Apostille.¹⁰⁵ The Convention does not specify a limited period of validity of the Apostille, but it also does not prevent contracting states from establishing such time limits if they choose to do so.¹⁰⁶

When it comes to the application of the Apostille Convention to electronic documents and their printouts, there are various comparative approaches that can be found. Austria consistently applies a dual approach when adding Apostilles to public documents. A physical (paper) Apostille is exclusively attached to physical public documents, while only an e-Apostille is issued on electronic public documents.¹⁰⁷ Similarly to Austria, Slovenia adds an e-Apostille to electronic public documents, but it is also possible to add an e-Apostille to a scanned copy of a public document in paper form, provided that the scanning

101 Apostille Handbook (n 87) 85

102 Yvon Loussouarn, *Explanatory Report on the Hague Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents* (HCCH 1961), paras 42–45.

103 Apostille Handbook (n 87) 37.

104 Loussouarn (n 102), paras 1–6.

105 Apostille Handbook (n 87) 89–90.

106 *ibid* 32.

107 HCCH, 'Austria - Apostille Questionnaire 2021' (2021) 5 <<https://assets.hcch.net/docs/c1d754e7-0fec-41a6-b203-f93c2a688c26.pdf>> accessed 20 January 2024.

was done by an authorised official.¹⁰⁸ On the other hand, countries like the Czech Republic and Portugal (none of which issue e-Apostilles) attach a traditional physical (paper) Apostille to printouts of electronic public documents.¹⁰⁹ In principle, according to the views of the Hague Conference, it is possible to add an Apostille to a printout of an electronic public document. However, the Hague Conference does not endorse this practice because the entire added value associated with the electronic form of the document is lost by printing an electronic public document on paper.¹¹⁰ In other words, an electronic document printed in this way, to which an Apostille has been added, will not have a machine-readable form after rescanning.¹¹¹

The Republic of Croatia does not issue a physical (paper) Apostille for Croatian electronic public documents because they are signed electronically. In addition, Croatia does not issue an Apostille for printouts of electronic public documents either because according to the opinion of the Croatian authority that filled out the Hague Conference questionnaire, such printouts are considered ordinary copies of the documents, not certified copies for which an Apostille would typically be issued.¹¹² From the perspective of the current normative situation, the argumentation provided by the Republic of Croatia in the Hague Conference questionnaire for 2021 is not sustainable. A printed electronic notarial document, without any additional certification, has the power of a certified copy of a notarial document, provided that such a printout contains a barcode or QR code, a control number and a website for verifying the authenticity of the document and downloading the original document.¹¹³ The legal equivalence of the printed electronic notarial document and a certified copy enables printed documents to replace the original notarial documents in legal circulation.¹¹⁴ In this context, certified copies of notarial documents *ex*

108 HCCH, 'Republic of Slovenia - Apostille Questionnaire 2021' (2021) 5 <<https://assets.hcch.net/docs/0b00bffe-82b8-4f0d-a833-e082837351f0.pdf>> accessed 20 January 2024.

109 HCCH, 'Implementation Chart of the e-APP' <<https://assets.hcch.net/docs/b697a1f1-13be-47a0-ab7e-96fcb750ed29.pdf>> accessed 20 January 2024; HCCH, 'Portugal - Apostille Questionnaire 2021' (2021) 4 <<https://assets.hcch.net/docs/f0f19d49-6a11-4263-bed9-7f4128d8927c.pdf>> accessed 20 January 2024; HCCH, 'Czech Republic - Apostille Questionnaire 2021' (2021) 6 <<https://assets.hcch.net/docs/eeeb3b9a-6a30-483d-a91d-ea3b420d3a3f.pdf>> accessed 20 January 2024.

110 Apostille Handbook (n 87) 73.

111 According to art 5(10) of the Act on the Right to Access Information, Official Gazette, Nos 25/13, 85/15, 69/22, a machine-readable format is defined as a file format structured in a manner that enables a software application to easily identify, recognize, and extract specific data from it, including individual data and their internal structure.

112 HCCH, 'Republic of Croatia - Apostille Questionnaire 2021' (2021) 6 <<https://assets.hcch.net/docs/a6f93f23-8074-4aaa-8cdf-64260107ef96.pdf>> accessed 20 January 2024.

113 NP Act, art 50a(2).

114 *ibid* art 95(2).

lege have the status of public documents.¹¹⁵ The aforementioned argumentation is not sustainable even in relation to the printed electronic court document (a judgment, a decision, etc.), which is signed/certified by a qualified electronic signature/seal and which contains a barcode or QR code, a control number and a website for verifying the authenticity of the document and downloading the original document, since it also has the meaning of a certified copy in legal traffic, which is, within the meaning of art 230 of the CPA, a public document *per se*.¹¹⁶ Printed electronic public administration records obtained eg through the e-Citizens system also have the status of public documents, provided that they contain a record number and a control number in order to check the authenticity of the record by checking the original electronic record via the website.¹¹⁷ However, in relation to the latter, ie printed electronic public administration records, it should be borne in mind that they have a limited legal lifespan.¹¹⁸ After a period of three months, an electronic record generated for verification is deleted from the system, and it is no longer possible to verify the authenticity of the printed electronic record.¹¹⁹ Consequently, an electronic record printed on paper loses its status of public document, ie it is no longer legally valid.¹²⁰ Therefore, it is to be assumed that even an Apostille on such a document would lose its legal effect because it would be on a document that does not have the status of public document or that has lost its legal effect. In that case, for people who intend to use a Croatian public document abroad, for the sake of legal certainty, it would still be advisable to obtain a public document in paper form with a handwritten signature of an authorised person and a printed physical seal of the public document issuer. In that case, by the mere passage of time, a public document would not cease to exist, ie it would not lose its legal effect, nor could it be considered that an Apostille was added to a document that is not a public document.

Furthermore, any justification that the receiving country's authority can verify the authenticity of a Croatian public document by entering control numbers or scanning QR codes on the printed electronic public document would represent a transfer of responsibility for authenticity verification to the document receiving country. This, in turn, contradicts the Apostille Convention, as it is the duty of the issuing country to verify the authenticity of a public document,

115 *ibid* art 3(2).

116 Court Rules of Procedure, Official Gazette, Nos 37/14, 49/14, 8/15, 35/15, 123/15, 45/16, 29/17, 33/17, 34/17, 57/17, 101/18, 119/18, 81/19, 128/19, 39/20, 47/20, 138/20, 147/20, 70/21, 99/21, 145/21, 23/22, 12/23, 122/23, arts 1a(2) and 65(3)(4).

117 Regulation on Organisational and Technical Standards for Connecting to the National Information Infrastructure, Official Gazette, No 60/17, art 15(1)–(3).

118 See n 69.

119 Regulation on Organisational and Technical Standards for Connecting to the National Information Infrastructure, Official Gazette, No 60/17, art 15(4).

120 *ibid* art 15(1)–(4).

unless according to the law of the receiving country or based on an international treaty, the public document of the issuing country is exempt from legalisation or similar formality.¹²¹ It is also important to note that, in addition to verifying the authenticity of the signature and seal or stamp, the Apostille also confirms the capacity in which the person signing the document acted (a judge, a government official, etc.).¹²²

Namely, according to the eIDAS Regulation,¹²³ a qualified electronic signature has the same legal effect as a handwritten signature.¹²⁴ It follows from the above that the legal effects are such that the existence of a signature on a document could not be contested simply because the document contains a qualified electronic signature. In relation to the qualified electronic seal, the Regulation introduces the presumption of data integrity and of correctness of the origin of that data to which the qualified electronic seal is linked.¹²⁵ No less important, it should also be borne in mind that the territorial application of the eIDAS Regulation is limited to EU Member States, hence the Regulation is not applicable to all parties to the Apostille Convention, of which there are significantly more.¹²⁶

On the other hand, there is the question of the use of foreign electronic public documents before Croatian courts. Pursuant to the CPA, all documents attached to the submission, regardless of whether they are public or private, shall be submitted in the original or as a copy.¹²⁷ With regard to electronic documents, a public document should certainly be considered in the first place a document originally drawn up in electronic form, while a printout of an electronic public document, ie whether such printout is also considered a public document, will be judged according to the *lex loci actus*.¹²⁸ In German civil procedural law, the presumption of authenticity is attached to electronic public documents signed with a qualified electronic signature, as well as to documents in paper (physical) form.¹²⁹ However, according to the prevailing opinion, this presumption in German law does not apply to foreign electronic public documents.¹³⁰ The understanding of German civil procedural law is comparable to

121 Apostille Convention, arts 1(1), 3, 5 and 6.

122 Apostille Handbook (n 87) 31.

123 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257 (hereinafter referred to as 'the eIDAS Regulation').

124 eIDAS Regulation, art 25(2).

125 *ibid* art 35(2).

126 *ibid* art 52.

127 CPA, art 108(1).

128 Apostille Handbook (n 87) 58.

129 Nazrin Hasanova, 'The Electronic Apostille in Worldwide Circulation of Public Documents' (2023) 9(1) Baku State University Law Review 23, 34.

130 *ibid* 34–35.

Croatian civil procedural law. Although the CPA does not contain an explicit norm in terms of the presumption of authenticity of electronic public documents, a comparable situation is reached in a different way. Namely, the Croatian legislator decided to explicitly attribute the status of public document to certain electronic documents, which consequently encompasses all legal consequences of the status of such a document within the meaning of the CPA. Thus, the authenticity of foreign electronic public documents could not be presumed even according to Croatian civil procedural law, and this is because the CPA, as a general assumption of the use of foreign public documents, requires proper certification in any case, unless otherwise stipulated by international treaties, and in doing so, the CPA makes no distinction regarding the form of foreign public documents.¹³¹

Of all the Hague Conventions, the Apostille Convention appears most often in practice. It is precisely this frequency of application and the constantly growing number of contracting parties that impose the question of adapting this regime to the modern digitalised national judicial apparatus and digitalised cross-border judicial cooperation. Since the Convention was drafted half a century ago in a technology-neutral way, it can continue to operate even in changed circumstances. At the same time, new technologies can improve and increase efficiency and legal security in the legalisation of foreign public documents.

Guided by this, the Hague Conference on Private International Law and the National Notary Association of the USA initiated the e-APP programme in 2006.¹³² The e-APP has two components, e-Apostilles and e-Registers. Although the full effect would be best achieved by the comparative application of both components, a greater number of contracting parties to this Convention have only accessed the e-Register. There are numerous advantages of the electronic version of the Apostille. The use of modern technology introduces a fast and secure way of working, with many tools to combat fraud and Apostille abuse. At the same time, it also standardises the working methods of competent authorities and leads to greater accessibility for users. According to the latest data, approximately 10% of all Apostilles are e-Apostilles, with this figure constantly growing.¹³³ Numerous advantages are also associated with the e-Register. Storing Apostilles in the e-Register reduces the need for official intervention since verification of issued Apostilles is available at any time in the system.

¹³¹ CPA, art 231.

¹³² Hans Van Loon, 'The Hague Conference on Private International Law: Work in Progress (2003-2004)' [2005] *Yearbook of Private International Law* 237, 245.

¹³³ HCCH, '12th International Forum on the electronic Apostille Program (e-APP)' (2021) 12 <<https://www.hcch.net/en/instruments/specialised-sections/apostille/international-forum-eapp/>> accessed 21 January 2024.

An e-Apostille is a certificate referred to in art 3(1) of the Apostille Convention, which is issued in electronic form and signed with a digital signature. An e-Apostille supports both electronic public documents and paper public documents that have been scanned into electronic form or digitised.¹³⁴ All formal requirements defined by the Convention for an Apostille must also be met when it comes to an e-Apostille. In order to issue an e-Apostille, the contracting party must have appropriate technology and software for creating an e-Apostille and an electronic transmission mechanism. The competent authority must also have access to digital signature certificates.

In order for the competent authority of the country issuing the public document to digitally sign and attach the e-Apostille, that authority shall possess a digital certificate issued by a reliable trust service provider.¹³⁵ Namely, any mark, symbol or name that appears on a document in electronic form and is authenticated by means of a digital certificate to evidence the signing of that document can be considered a digital signature.¹³⁶ In this case, the certificate acts as an electronic credential that links the identity of the signature to an individual or authority through public key infrastructure.¹³⁷

In respect of e-Apostille transmission, we distinguish between dynamic transmission, where the competent authority sends an e-Apostille electronically, and static transmission, where an e-Apostille is stored in an e-Register that is accessible to users. The rules laid down in art 7 of the Convention apply to the e-Register, as in the case of the classic register.

The contracting states should organise the use of the e-Apostille system in accordance with the basic principles adopted by the Special Commission in 2021. Accordingly, 1) e-Apostille and related services should be accessible to all users, 2) the competent authority should maintain the integrity of the e-Apostille and the public document it certifies, 3) e-Registers speed up the procedure and increase legal certainty in terms of the database of Apostilles that have been issued, 4) contracting parties should develop mechanisms to facilitate the acceptance of e-Apostilles, and 5) the competent authority systematically updates and upgrades its Apostille related practices as well as the e-Apostille infrastructure.¹³⁸

134 Apostille Handbook (n 87) 97.

135 *ibid* 332.

136 *ibid* 17.

137 *ibid*.

138 HCCH, 'The e-APP: Key Principles and Good Practices' (2021) <<https://assets.hcch.net/docs/ff855998-d234-485c-a6c9-f705c8c692e6.pdf>> accessed 21 January 2024.

3.4 EU regimes for the circulation of public documents

The status of certain public documents originating from EU Member States is defined by the Regulation on Public Documents.¹³⁹ The purpose of the Regulation on Public Documents is to simplify the circulation of public documents between the Member States and certified copies thereof within the EU, which are issued by the authorities of one Member State and are to be used before the authorities of another Member State in such a way that certain documents are exempt from all forms of legalisation and similar formality, ie an Apostille is added in terms of the Apostille Convention.¹⁴⁰ The Regulation contributes to the further strengthening of freedom of movement within the EU by facilitating the use of public documents issued in one Member State, which prove certain facts before the authorities of other Member States.¹⁴¹ Public documents issued by the third-country authorities, as well as certified copies thereof certified by the authority of a Member State, are excluded from the scope of the Regulation on Public Documents.¹⁴²

In terms of the Regulation on Public Documents, public documents are considered to be documents issued by an authority or court official of a Member State (including documents issued by the state attorney's office, the head of the court register office or a bailiff), administrative documents, notarial documents, official certificates placed on private documents (official certificates recording the registration of a document or the fact that it was in existence on a certain date, and official and notarial authentications of signatures), and documents drawn up by the diplomatic or consular agents of a Member State in the territory of any state, where such documents have to be presented in the territory of another Member State or to the diplomatic or consular agents of another Member State acting in the territory of a third state.¹⁴³ The Regulation on Public Documents opts for the criterion of the legal order based on which the issuer acquired public powers, and within the scope of the Regulation, a public document is considered to be a document issued by the authority of a Member State in accordance with its national law, which needs to be presented to the authorities of another Member State, and this also includes the documents of the diplomatic or consular agents of Member States.¹⁴⁴ It is clear from the above that the definition of public documents within the meaning of the

139 Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No 1024/2012 [2016] OJ L200 (hereinafter referred to as 'the Regulation on Public Documents').

140 Regulation on Public Documents, arts 1(1) and 4.

141 Stefan Schlauß, 'The EU Regulation on Public Documents: A first step towards the abolition of the Apostille in the EU' (2020) 21 ERA Forum 117, 118.

142 Regulation on Public Documents, art 2(3).

143 *ibid* art 3(1).

144 *ibid* arts 2(1) and 3(1).

Regulation on Public Documents has a wider scope compared to the definition of public documents pursuant to the Apostille Convention due to the fact that the Regulation on Public Documents also includes documents executed by diplomatic or consular agents of Member States, while the Apostille Convention does not apply to documents executed by diplomatic or consular agents.¹⁴⁵

However, the Regulation on Public Documents applies exclusively to those public documents of Member States that establish one or more of the following facts: birth; that a person is alive; death; name; marriage, including capacity to marry and marital status; divorce, legal separation or marriage annulment; registered partnership, including capacity to enter into a registered partnership and registered partnership status; dissolution of a registered partnership, legal separation or annulment of a registered partnership; parenthood; adoption; domicile and/or residence; nationality; absence of a criminal record, provided that public documents establishing this fact are issued for an EU citizen by the authority of that citizen's Member State of nationality, and to public documents, the presentation of which may be required of EU citizens residing in a Member State of which they are not nationals when they wish to vote or stand as candidates in local elections or elections to the European Parliament.¹⁴⁶

Although the Regulation on Public Documents introduces a liberal approach in terms of exemption from legalisation or the addition of an Apostille to certain public documents that prove certain facts, the Regulation also prescribes protective mechanisms due to doubts as to the authenticity of a public document issued by the authority of another Member State. Thus, the Regulation relies on the already existing Internal Market Information System (hereinafter referred to as 'IMI'), which is used as a communication platform between Member States in the field of administrative cross-border cooperation.¹⁴⁷ Through the IMI system, the Member State authorities can compare presented public documents or certified copies thereof with models of document that are normally issued in the issuing Member State, and they can also communicate with the authorities or the central authority of the issuing state.¹⁴⁸ Direct communication with the issuing country is recommended in any case whenever there is doubt as to the authenticity of the signature or seal, the capacity in which the person signing the document has acted, and forgery or subsequent unauthorised alteration of the document.¹⁴⁹

In addition, the Regulation on Public Documents also simplifies other formalities in the circulation of public documents, which fall within the scope

145 cf Regulation on Public Documents, art 3(1) and Apostille Convention, art 1(3).

146 Regulation on Public Documents, art 2(1)(2).

147 Schlauß (n 141) 125.

148 Cristina Campiglio, 'Circulation of Public Documents and Recognition of Civil Status Situations – Lights and Shadows' [2021/2022] *Yearbook of Private International Law* 1, 9.

149 Regulation on Public Documents, art 14(1)(2); Schlauß (n 141) 125.

of the Regulation. Thus, it is prescribed that certified copies of public documents made in one Member State are accepted in another Member State if that Member State otherwise accepts certified copies of public documents according to its law.¹⁵⁰ Likewise, if a Member State requires the presentation of the original of a public document issued by the authorities of another Member State, the authorities of the Member State where the public document is presented do not also require the presentation of a certified copy thereof.¹⁵¹ In addition to the aforementioned, the Regulation additionally facilitates the use of public documents from the aspect of linguistic pluralism within the EU. Thus, the Regulation introduces the possibility of using multilingual standard forms that have no autonomous legal value and are attached to public documents as aids, at the request of a person, to avoid the need to translate public documents and the associated costs.¹⁵² However, the use of multilingual forms is limited such that the forms exist only for documents that prove specific facts and not all facts that fall within the scope of the Regulation, so ultimately it will still be necessary to provide a translation for certain types of documents.¹⁵³ In view of the advanced digitalisation, templates of multilingual standard forms are available on the European e-Justice Portal in electronic form for each Member State to enable the online filling of forms or their download to a personal computer.¹⁵⁴ In this regard, it should be emphasised that the Regulation also applies to electronic public documents; however, it will ultimately depend on the national procedural autonomy whether such an electronic public document will be accepted, ie whether it can be used as electronic evidence according to the *lex fori*.¹⁵⁵ Although the Regulation on Public Documents undoubtedly contributes to a simpler circulation of public documents within the EU, the aforementioned could be facilitated further, provided that Member States digitise civil status data on persons by connecting the interoperable national civil status records of all Member State, which would create an interconnected network state registries within the EU.¹⁵⁶

Following the above, it should be noted that a simplified circulation of certain public documents within the EU based on the Regulation on Public Documents does not in any way affect the recognition of legal effects related to the content of public documents in the Member State in which a certain public document is to be used.¹⁵⁷ From the perspective of Croatian law, the afore-

150 Regulation on Public Documents, art 5(2).

151 *ibid* art 5(1).

152 *ibid* arts 6(1), 7(1) and 8(1).

153 Schlauß (n 141) 122.

154 Regulation on Public Documents, art 12; Schlauß (n 141) 123.

155 *ibid* recital n 9.

156 Campiglio (n 148) 10.

157 Regulation on Public Documents, art 2(4).

mentioned means that certain public documents issued by authorities of other Member States will be exempted from legalisation and addition of an Apostille before Croatian authorities, and will have evidentiary value in accordance with domestic procedural regulations. Specifically, from the aspect of civil procedural law, in terms of evidentiary value, they will be equivalent to domestic public documents.¹⁵⁸ Given that the Regulation on Public Documents does not impose a duty on the Member State receiving the document to recognise the public document of another Member State in the substantive sense, their recognition will depend on the national law of individual Member States, unless otherwise stipulated by international treaties.¹⁵⁹ Thus, in the Republic of Croatia, the facts of birth, marriage or death of Croatian citizens born abroad are registered on the basis of a state registry extract of a foreign authority.¹⁶⁰ Specifically, if we bring the previous national law provision into connection with the Regulation on Public Documents, it follows from the above that according to Croatian law, state registry extracts, which prove the facts of birth, marriage or death of Croatian citizens established in another Member State, which were issued by the authorities of the Member States within the framework of the Regulation on Public Documents, without the need for legalisation or the addition of an Apostille, ultimately result in legal effects in the Republic of Croatia, ie registration in a specific state registry such as a civil register. In relation to the application of public civil status documents issued within the framework of the Regulation on Public Documents, it should be emphasised that it in no way limits citizens, but moreover, citizens have the right to use other public documents that prove certain civil status, which are issued within the framework of the International Commission on Civil Status conventions if the Member States issuing and receiving the public document are parties to a certain convention.¹⁶¹

When it comes to the importance of the Regulation on Public Documents in terms of the simplified circulation of public documents within the EU, it should be noted that in 2023 the European Commission published a Proposal for a Directive to further expand and upgrade the use of digital tools and processes in company law.¹⁶² The Directive, *inter alia*, requires Member States to abolish legalisation or similar formality (Apostille) for copies and extracts of documents, including certified translations, of the court registers in Member States, but also for electronic copies and extracts of documents and translations

158 CPA, art 231.

159 Fitchen (n 89) 96.

160 SR Act, art 40(1).

161 Schlauß (n 141) 122.

162 Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law' COM (2023) 177 final (hereinafter referred to as 'the Proposal for a Directive on the Digitalisation of Company Law').

if they are authenticated by trust services within the meaning of the eIDAS Regulation.¹⁶³ Exemption from legalisation or the addition of an Apostille is also proposed for paper copies if they include the date of issuance as well as the seal or stamp of the register and have a feature that enables electronic verification of the authenticity of the document, such as a unique protocol or identification number.¹⁶⁴ It is important to point out that Member States have already been obliged to ensure that electronic copies and extracts of court register documents are authenticated by trust services in accordance with the eIDAS Regulation.¹⁶⁵ However, apparently the existing proposal of the Directive aims to further exempt authenticated documents from legalisation and obtaining an Apostille.

Additionally, this exemption from legalisation or the addition of an Apostille is proposed for notarial and administrative documents, their certified copies and translations in terms of cross-border procedures related to commercial companies, and it also applies to electronic notarial and administrative documents, their certified copies and translations if they are authenticated within the meaning of the eIDAS Regulation, and to those in paper form if they have a feature that enables electronic verification of the authenticity of the document.¹⁶⁶ Furthermore, the Directive introduces a digital EU power of attorney, for which it also prescribes exemption from legalisation or similar formalities such as the adding of an Apostille.¹⁶⁷ In order to carry out procedures in another Member State, companies will be able to use a standard model of the digital EU power of attorney to authorise a person to represent the company, and consequently it shall be accepted as evidence of the authorised person's entitlement to represent the company as specified in the power of attorney.¹⁶⁸ The condition for applying the digital power of attorney is that it is authenticated by trust services within the meaning of the eIDAS Regulation, ie that it is signed with an electronic qualified signature.¹⁶⁹

As regards the Proposal for a Directive on the digitalisation of company law, it is significant that legalisation or the addition of an Apostille is abolished only for certain documents in the context of cross-border procedures related to companies, provided that the electronic document is signed with a qualified electronic signature within the meaning of the eIDAS Regulation. A principle conclusion that emerges from the above, which is in general applicable to

¹⁶³ *ibid* art 16d(1).

¹⁶⁴ *ibid*.

¹⁶⁵ Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) [2017] OJ L169, art 16(4).

¹⁶⁶ Proposal for a Directive on the Digitalisation of Company Law, art 16d(3).

¹⁶⁷ *ibid* art 16d(2).

¹⁶⁸ *ibid* art 16c(1)(2).

¹⁶⁹ *ibid* art 16c(1).

cross-border legal traffic within the EU, is that the application of a qualified electronic signature or seal *per se* does not imply exemption of public documents from legalisation or the addition of an Apostille, but is an additional assumption that certain categories of public documents are exempt from legalisation or the addition of an Apostille by European norms. Namely, the eIDAS Regulation contains no general norm on the basis of which all types of public documents signed/certified with a qualified electronic signature/seal would be exempt from legalisation or the addition of an Apostille in cross-border legal traffic, but rather, as in the example of the Directive on the digitalisation of company law or the Regulation on Public Documents, exemption from legalisation or the addition of an Apostille is laid down for certain categories of public documents.

In terms of the registration in the state registries of the Republic of Croatia of the fact of divorce or marriage annulment, which was decided by the court of another Member State, it should be noted that even for this, no special procedure for updating the state registry will be necessary since under the Brussels II ter Regulation,¹⁷⁰ the decision *res judicata* of the court of one Member State, as a public document, directly produces effects in another Member State without the need for a special recognition procedure, and without the need for legalisation or similar formality of the court decision in question.¹⁷¹ However, as already mentioned, such legal effects of the decision in the matrimonial dispute arise on the basis of the Brussels II ter Regulation, and not on the basis of the Regulation on Public Documents. Namely, with regard to the relationship between the instruments of the European Private International Law (hereinafter referred to as ‘EU-PIL’) and the Regulation on Public Documents, it was clarified that the Regulation is a horizontal instrument complementary to EU-PIL instruments (such as the Brussels II ter Regulation), while some of them, which eg specifically regulate the issues of the recognition of professional qualifications, will even have an advantage in terms of the application in relation thereto.¹⁷²

170 Council Regulation (EU) 2019/1111 of 25 June 2019 on jurisdiction, the recognition and enforcement of decisions in matrimonial matters and the matters of parental responsibility, and on international child abduction (recast) [2019] OJ L178 (hereinafter referred to as ‘the Brussels II ter Regulation’).

171 Ilaria Pretelli, ‘Article 30 – Recognition of a Decision’ in Cristina González Beilfuss and others (eds), *Jurisdiction, Recognition and Enforcement in Matrimonial and Parental Responsibility Matters - A Commentary on Regulation 2019/1111 (Brussels IIb)* (Edward Elgar Publishing 2023) 328; Brussels II ter Regulation, arts 30(1)(2) and 90.

172 HCCH, ‘EU answers to the questionnaire on the practical operation of the Hague Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Documents (Apostille Convention)’ (2021) <<https://assets.hcch.net/docs/799b6765-4d4f-44b9-900f-45ce637edb81.pdf>> accessed 20 January 2024.

Further to the above, it is generally necessary to consider the use of foreign court decisions as public documents of one Member State before the authorities of another Member State. Namely, based on EU-PIL instruments, the decision of a court of a Member State in certain matters is recognised in another Member State, with no special procedure for the recognition and enforcement of the decision in question.¹⁷³ Or simply put, it is a system of mutual automatic recognition of decisions of EU Member States, based on the principle of mutual recognition, whose legal basis relies on the founding treaties of the EU, and whose purpose is to ensure the smooth circulation of court decisions in civil and commercial matters between EU Member States.¹⁷⁴ As regards decisions made by applying specific instruments, which are to be used in another Member State, EU-PIL instruments provide for exemption from legalisation or other formalities.¹⁷⁵

At the same time, it is necessary to understand that such recognition of decisions of Member States in the regime of EU-PIL instruments refers to their specific effect as legal acts, which are equal in effect to the decisions of domestic courts.

However, we should distinguish from that situations in which the decisions made by applying EU-PIL instruments will be used exclusively for the purpose of proving a certain fact, ie as a means of proof, within the framework of a certain legal protection procedure before the authorities of another Member State different from the country of origin of the decision. Is it considered that such a decision represents a means of proof without the need to certify it with an Apostille?

Pursuant to the Brussels I bis Regulation, if for any reason, a party wishes to invoke the effects of a court decision given in another Member State before the authorities of another Member State, the decision in question should be accompanied by a 'Certificate concerning a judgment in civil and commercial matters', which is, based on the Regulation, issued by the court of origin that has given the judgment at the request of the interested party.¹⁷⁶ Additionally, the

173 See, eg, Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351 (hereinafter referred to as 'the Brussels I bis Regulation'), art 36(1); Brussels II ter Regulation, art 30(1); Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L201, art 39(1).

174 Mirela Župan, '50 godina europske pravosudne suradnje u građanskim stvarima – 5 godina hrvatske primjene' (2019) 10(1) *Godišnjak Akademije pravnih znanosti Hrvatske* 469, 473; Ines Medić, 'Priznanje i ovrha na području EU' (2017) 54(1) *Zbornik radova Pravnog fakulteta u Splitu* 283, 291–292.

175 See Brussels I bis Regulation, art 61 and Brussels II ter Regulation, art 90.

176 Brussels I bis Regulation, arts 37(1) and 53.

Brussels I bis Regulation stipulates that legalisation or other similar formality is not required for documents issued in a Member State under the Regulation.¹⁷⁷ Therefore, such documents are entirely exempt from both legalisation and the addition of an Apostille. However, the question arises as to the meaning of the wording '*document ... issued within the framework of this Regulation*', or more precisely, if the above wording refers to all types of documents, including judgments, or only to documents whose issuance is prescribed by the Regulation, such as the aforementioned certificate concerning a judgment and a certificate concerning an authentic instrument/court settlement, whose forms are attached to the Regulation and form an integral part thereof.¹⁷⁸ Relevant legal theory does not provide unequivocal answers since in relation to the provision of art 61 of the Brussels I bis Regulation it underlines the importance of the certificates provided for in annexes I and II, and merely states that no additional review or special formality of anything issued under that regulation is necessary.¹⁷⁹

On the other hand, the Brussels II ter Regulation uses a somewhat broader wording and stipulates that '*no legalisation or any other similar formality is required in the context of this Regulation*'.¹⁸⁰ In terms of the Brussels II ter Regulation, the above applies equally to judgments and other court decisions, but also to all other documents issued under the Brussels II ter Regulation.¹⁸¹ The Brussels II ter Regulation also stipulates that, in addition to the decision in question, a party who wishes to invoke the effects of a decision given in the Member State of origin before the authorities of another Member State must also attach certain certificates, depending on the specific legal matter (Certificate concerning decisions in matrimonial matters, Certificate concerning decisions in matters of parental responsibility, Certificate concerning decisions ordering the return of a child to another Member State, etc.).¹⁸²

Although the certificates in question, which are attached to the Brussels I bis Regulation and the Brussels II ter Regulation, have different functions, their common purpose is to ensure that the authority of the Member State receiving the decision assures that the court decision of the Member State of origin is true, ie authentic.¹⁸³ However, exemption from legalisation or the addition of an Apostille should not be taken without reservation. Namely, as the Brussels I bis

¹⁷⁷ *ibid* art 61.

¹⁷⁸ *ibid* annexes I and II.

¹⁷⁹ Martin George and others, 'General Provisions' in Andrew Dickinson and Eva Lein (eds), *The Brussels I Regulation Recast* (OUP 2015) 542.

¹⁸⁰ Brussels II ter Regulation, art 90.

¹⁸¹ Thalia Kruger, 'Article 90 – Legalisation or other similar formality' in Cristina González Beilfuss and others (eds), *Jurisdiction, Recognition and Enforcement in Matrimonial and Parental Responsibility Matters - A Commentary on Regulation 2019/1111 (Brussels IIb)* (Edward Elgar Publishing 2023) 629.

¹⁸² Brussels II ter Regulation, arts 31(1) and 36(1). See annexes to the Brussels II ter Regulation.

¹⁸³ Kruger (n 181) 632.

Regulation and the Brussels II ter Regulation exempt only decisions and other documents within the framework of these regulations from legalisation or similar formality, it should be noted that such exemption applies only within the scope of application of these regulations.¹⁸⁴ In other words, it should be understood that such exemption from legalisation or similar formality is applied only for the purpose of the recognition and enforcement in cross-border matters.¹⁸⁵ EU-PIL instruments, such as the Brussels I bis Regulation, provide exclusively a legal framework for mutual automatic recognition and enforcement of Member State decisions, ie the recognition of legal effects in another Member State, but EU-PIL instruments do not imply or have any effect on the evidentiary value of a court decision of one Member State before the court of another Member State when the decision is used as proof of fact, and the evidentiary proceeding issues, including the assumptions about the use of certain means of proof, should be evaluated according to the *lex fori*.¹⁸⁶ From the perspective of Croatian civil procedural law, a court decision given by another Member State, if used exclusively as a means of proof, should have an Apostille, given that all EU Member States are also parties to the Apostille Convention, unless total exemption from certification of public documents between the Republic of Croatia and the Member State of origin of the document is stipulated by some other international treaty.¹⁸⁷

Hence, it is necessary to distinguish between two legal situations. The first one would refer to the need of a party to raise an objection *res judicata* within the framework of the proceedings before the court of a Member State that is different from the Member State of origin of the decision. Here, one should start from the effect of a foreign decision to which certain legal presumptions of different effect are attached. Specifically, in terms of the objection *res judicata*, one should start from the fact that the wording of the decision *res judicata* represents a legal disposition of the court, and as such, it expresses a certain legal situation, and in no way is this about using the decision as a means of proof in the sense of the usual understanding.¹⁸⁸ Therefore, in order to emphasise the objection *res judicata*, the decision should be accompanied by an adequate certificate in terms of the Brussels I bis Regulation and the Brussels II ter Regulation. However, this obligation to attach a certificate does not apply to those cases when a court decision is used as a means of proof in the

184 Xandra Kramer, 'Article 61' in Ulrich Magnus and Peter Mankowski (eds), *Brussels I bis Regulation* (Verlag Dr. Otto Schmidt 2023) 956.

185 George (n 179) 541–542.

186 Pietro Franzina and others, 'The Recognition and Enforcement of Member State Judgments' in Andrew Dickinson and Eva Lein (eds), *The Brussels I Regulation Recast* (OUP 2015) 376.

187 HCCH, 'Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents - Status table' (2024) <<https://www.hcch.net/en/instruments/conventions/status-table/?cid=41>> accessed 18 January 2024.

188 Franzina (n 186) 376.

evidentiary proceeding to prove the facts.¹⁸⁹ Nevertheless, in accordance with the understanding of the prevailing procedural law theory, if a foreign decision is treated as an 'ordinary' public document, ie if it is not recognised, it would have to be at least legalised in order to attach the presumption of authenticity thereto. Otherwise, by resorting to the principle of free evaluation of evidence, an unrecognised and non-legalised decision could be recognised to have a greater effect than it actually has, assuming it is a decision made between parties, possibly of a certain content, but from the perspective of the Croatian legal system, it is non-existent.¹⁹⁰

In this regard, if the decision of the court of a Member State before the court of another Member State is used exclusively as a means of proof, from the aspect of efficiency and effectiveness in proceedings, it would be opportune to make an exception in relation to those decisions of the court of other Member States with prescribed certificates within the meaning of EU-PIL regulations. Namely, if they are automatically recognised as having legal effects, it should be considered that they can also be taken as duly authenticated foreign public documents within the meaning of the CPA, without the need for adding an Apostille.

In terms of comparative arrangements, it should be stressed that the German legal system does not provide for special rules regulating the status of public documents exempt from legalisation under EU law, but general national rules apply. Accordingly, as regards the admissibility of this evidentiary value, German law equates foreign public documents under the regime of either the Apostille Convention, bilateral treaties or EU-PIL instruments with documents issued in Germany.

As regards non-legalised public documents, § 438(1) of the Code of Civil Procedure (hereinafter referred to as 'the CCP') leaves this matter at the discretion of the court to assess whether a foreign public document can be considered authentic without additional evidence thereof. This excludes situations in which foreign public documents are exempt from legalisation under the regime of EU-PIL instruments. In all other situations, the court will require the necessary information on the authenticity of the foreign public document to be delivered by the competent authorities (German embassies, consulates, Landesarbeitsgericht Hamm). If under § 438(1) of the CCP the court assesses that such a foreign document is authentic, such a document is recognised under §§ 415 et seq. of the CCP as having the same evidentiary value as German public documents (see the decision of the Bundesverwaltungsgericht, NJW 1987, p. 1159, and the decision of the Bundesgerichtshof, BGH LM § 418 of the CCP

¹⁸⁹ *ibid* 393.

¹⁹⁰ Dika (n 4) 543.

No. 3). However, the assessment of the authenticity of the content of a foreign public document in that case is at the discretion of the court.

In respect of court decisions of other Member States that are accompanied by prescribed certificates within the meaning of EU-PIL regulations as foreign public documents, the prevailing German legal theory also agrees with liberalisation in terms of the necessity of the addition of an Apostille or legalisation. However, it also warns that such a step should be accompanied by the resolution of doubts in relation to the interpretation of the court decision as a public document.¹⁹¹

Finally, in terms of the aforementioned regarding the absence of the rules of evidence in relation to certain EU-PIL instruments, attention should also be drawn to the opposite normative solutions. The Succession Regulation,¹⁹² which also provides for exemption from legalisation and other formalities (an Apostille) for documents of Member States, additionally explicitly regulates rules of evidence in respect of individual documents.¹⁹³ This refers to public documents and the European Certificate of Succession. Thus, for a public document drawn up in one Member State, it is prescribed that it has the same evidentiary value in another Member State as in the Member State of origin, or the most similar effect, provided that this is not obviously contrary to the public policy of the Member State in which the document is presented.¹⁹⁴ An important difference follows from the above in relation to the principle use of foreign public documents before the authorities of another state. Namely, a represented rule is that the evidentiary value of a foreign public document is assessed according to the *lex fori*; however, in the context of public documents, in accordance with the Succession Regulation, the court of a Member State will assess the evidentiary value of a public document according to the law of the issuing Member State, ie according to the *lex loci actus*.¹⁹⁵ Furthermore, with regard to the European Certificate of Succession, the authenticity of the Certificate is presumed. Consequently, it is assumed that the Certificate accurately proves the elements established by the law applicable to succession or by any other law applicable to certain elements, and that the person named in the Certificate

191 Burkhard Hess and others, *Legalisation of Public Documents within the EU Member States* (BIICL 2006).

192 Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L201 (hereinafter referred to as 'the Succession Regulation').

193 *ibid* recs 61 and 71; art 74.

194 *ibid* art 59(1).

195 Vuković and Kunštek (n 46) 203–204.

as the heir, legatee, executor of the will or administrator of the estate, has the status specified in the Certificate.¹⁹⁶

4. Court decision as a public document in the procedure of recognition of a foreign court decision on the basis of the PIL Act

Through a recent *ad hoc* legislative intervention, the PIL Act was amended in such a way that, *inter alia*, additional prerequisites have been prescribed for the recognition of a foreign court decision on the adoption of a child from a country that is not a party to the international treaty governing international adoption.¹⁹⁷

In this context, the provision of art 71a(1) of the PIL Act stipulates that such a foreign court decision on adoption will be recognised after the court verifies the authenticity of that decision through diplomatic channels, and if the applicant has provided proof of *res judicata* of the decision, and has also submitted proof of the legalisation of the adoption decision in accordance with the law governing the legalisation of documents in international legal traffic.¹⁹⁸ It follows from the above that the provision of art 71a(1) of the PIL Act applies to those foreign court decisions on adoption of a child from a country that is not a party to the international adoption treaty, and with which the Republic of Croatia has not concluded a bilateral or multilateral treaty regulating the circulation of public documents in a different way. Otherwise, if international legalisation of foreign documents were insisted upon according to the LPD Act, it would be contrary to the provisions of the Constitution of the Republic of Croatia on the legal force of international treaties, and it would also cause a violation of the international obligations of the Republic of Croatia.¹⁹⁹ Legislative intervention, as implemented by art 71a(1) of the PIL Act, is redundant for several reasons.

First, the legislator unnecessarily refers to mandatory verification of the authenticity of the decision on adoption through diplomatic channels, ie through the Croatian Ministry of Foreign and European Affairs, given that further in the provision of art 71a(1) of the PIL Act it prescribes the obligation to submit proof of the legalisation of a foreign court decision. However, regardless of that, the possibility of diplomatic verification of the authenticity of a foreign public document has already existed on the basis of the LPD Act such that if

196 Succession Regulation, art 69(2).

197 Act Amending the Private International Law Act, Official Gazette, No 67/23, art 1.

198 PIL Act, art 71a(1).

199 Constitution of the Republic of Croatia, Official Gazette, Nos 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14, art 134.

the authority to which a foreign public document is submitted has doubts as to the authenticity of the document, it can request the Ministry of Foreign and European Affairs to check whether the document was issued by the authority indicated therein.²⁰⁰ It can be assumed that the use of unauthentic documents is an exception, not the rule. However, the legislator has obviously decided on a different approach and introduced the assumption that obviously every foreign decision on the adoption of a child, which falls within the scope of art 71a(1) of the CPA, is by nature *indicium suspecta* and should therefore be checked through diplomatic channels. At the same time, this also renders the procedure of international legalisation, which is supposed to be conducted by the Ministry of Foreign and European Affairs, or diplomatic and consular representations of the Republic of Croatia abroad, meaningless for foreign public documents intended for use before the authorities of the Republic of Croatia.²⁰¹

Second, an intervention is redundant since proof of *res judicata* of a foreign court decision is obligatorily attached to the proposal for recognition in terms of the provisions of the PIL Act that have been in force.²⁰² Therefore, it was unnecessary in the provision of art 71a(1) of the PIL Act to emphasise the obligation to attach proof of *res judicata* of a foreign court decision on adoption because it must be attached whenever it comes to the recognition of a foreign court decision based on the PIL Act, regardless of the specific legal matter in the proceeding from which the foreign decision originates (adoption, divorce, payment of a monetary claim, etc.).²⁰³ From the provision of art 67(1) of the PIL Act before the legislative amendment in question, it was not clear that the applicant in the process of recognising a foreign court decision on adoption of a child would be exempt from the obligation to submit proof of *res judicata* of a foreign court decision. However, since the legislator has already decided to standardise in detail the procedure for the recognition of a foreign court decision on adoption of a child in the manner prescribed, it should be noted that addressees were not additionally instructed to pay attention to proof of *res judicata* of a foreign court decision. Namely, as a presumption of the recognition of a foreign court decision, the PIL Act prescribes the duty of the proposer, along with that decision, to submit proof of *res judicata* of that decision under the law of the country in which it was made.²⁰⁴ Although the earlier Act on the Resolution of Conflict of Laws with Regulations of Other Countries provides for the obligation to attach proof of *res judicata* as a formal act, the PIL Act is more flexible in certain cases and provides for the obligation to attach proof

200 LPD Act, art 4.

201 *ibid* art 3(1).

202 PIL Act, art 67(1).

203 See art 67(1) of the PIL Act.

204 PIL Act, art 67(1).

of *res judicata* of a foreign court decision.²⁰⁵ However, proof of *res judicata* of a foreign court decision is usually issued in the form of a clause printed on the decision itself, in the form of a special certificate or in the form of some other formal document.²⁰⁶

Namely, a certificate of *res judicata* of a foreign court decision could also be a public document *per se*, and since it originates from a foreign country, such an act could be considered a foreign public document.²⁰⁷ The authority issuing a certificate of *res judicata* may or may not be the same authority that made the specific court decision, and this depends on the law of the country of origin of the decision.²⁰⁸ Hence, the stamp and/or signature do not necessarily have to be the same as those found on the foreign court decision itself, ie placed at the time it was issued. The foregoing justifies that when recognising a foreign court decision, the status of a certificate of *res judicata* should also be considered according to the *lex loci actus*, and secondly Croatian law, or whether such an act is considered a separate foreign public document. Therefore, if the *lex loci actus* and in any case the subordinate Croatian law qualify the formal certificate of *res judicata* as a public document, it will be necessary to legalise it beforehand in terms of the LPD Act, unless otherwise stipulated by an international treaty.²⁰⁹ The PIL Act provides for the obligation to attach ‘proof of *res judicata* issued by the law of the court’, so the PIL Act qualifies as evidence any means whose purpose is to confirm the *res judicata* effect of a foreign court decision, regardless of whether it is a formal act or something else. All the more, if it is a formal act, then as evidence, such a public document should fulfil the general assumption about the use of a foreign public document as a means of proof within the meaning of the CPA and the LPD Act, ie that it is duly certified (legalised), unless otherwise stipulated by an international treaty.²¹⁰

However, in the event that a certificate of *res judicata* really has the status of foreign public document, there are certain limitations regarding the possibility of rebutting the presumption of authenticity, depending on the legal nature of a certificate of *res judicata* according to the law of the country of decision. This is because if a certificate of *res judicata* is treated as a separate court decision under the law of the country of decision, then in the recognition process, the legal dispositions of a foreign court in the act of the formality cannot be contradicted by applying the provision of art 230(3) of the CPA, ie it would not

205 cf Act on the Resolution of Conflict of Laws with Regulations of Other Countries, Official Gazette, Nos 53/91, 88/01, art 87 and PIL Act, art 67(1).

206 Vuković and Kunštek (n 46) 461.

207 *ibid* 461.

208 Mihajlo Dika, Gašo Knežević and Srđan Stojanović, *Komentar Zakona o međunarodnom privatnom pravu i procesnom pravu* (Nomos 1991) 286.

209 LPD Act, art 3; PIL Act, art 8(5).

210 CPA, art 231; LPD Act, art 3(1).

be allowed to prove falsehood of the act as a document in the direction that the presumption of *res judicata* were not fulfilled according to the law of the country of decision.²¹¹ This is because such a certificate could be challenged exclusively by legal means before the court of the decision, as is the case in Croatian civil proceedings, in which only the court that issued the domestic certificate of *res judicata* is authorised *ex officio* or at the request of the party to revoke it, provided that legal conditions for its issuance were not met.²¹² Thus, it can be concluded that a certificate of *res judicata*, as a specific court decision, can possibly be linked with a rebuttable presumption that a certificate of *res judicata* legally exists even after the adoption of a certificate of *res judicata* itself, ie that the court decision by its *lex fori* did not invalidate a certificate of *res judicata*.²¹³ In the event that a certificate of *res judicata* has in the meantime lost its legal effects, the opposing party could propose counter-evidence, ie prove that a certificate of *res judicata* does not exist as evidence. On the other hand, if a certificate of *res judicata* is considered exclusively a public document confirming the existence of a certain fact under the law of the country of decision, then a rebuttable presumption of authenticity would apply to such a document, and before the Croatian court it would be admissible to prove that the facts stated in the document are false, ie even to prove that the presumption of *res judicata* was not met according to the law of the country of decision.²¹⁴

Finally, thirdly, the reference from art 71a(1) of the PIL Act to the need to submit evidence of the legalisation of the decision on adoption is redundant since even before the legislative intervention in question, the aforementioned was a prerequisite for the recognition of each foreign court decision, including a decision on adopting a child, unless otherwise stipulated by an international treaty or European law.²¹⁵ Although the public nature of a foreign document in each individual case will still depend on the *lex loci actus* (art 3(3) of the LPD Act), and only secondarily on Croatian law, it should be assumed that, considering the legal force and authority of the state that stands behind a court decision, in the majority of legal systems they have the status of public documents. Consequently, a foreign public document can be used in the Republic of Croatia only if it is certified by the Ministry of Foreign and European Affairs, ie a diplomatic or consular representation of the Republic of Croatia abroad.²¹⁶ Given that the LPD Act uses the wording that public documents issued abroad ‘*can be used in the Republic of Croatia only if they are authenticated ...*’, this leads to the conclusion that the above applies to every use, without specifying whether

211 Dika, Knežević and Stojanović (n 208) 286.

212 Dika, Knežević and Stojanović (n 208) 286.; CPA, art 333a.

213 *Argumentum per analogiam* cf Dika (n 4) 532.

214 Dika, Knežević and Stojanović (n 208) 286.; CPA, arts 230(3) and 231.

215 Dika (n 4) 538.

216 LPD Act, art 3(1).

a foreign public document is used as a means of proof, as a mandatory attachment to the proposal for the recognition of a foreign court decision or for some other purpose. However, it must be concluded that the provision of the LPD Act primarily refers to the use of foreign public documents before the competent authorities of the Republic of Croatia and other persons with public power.

Furthermore, the provision of art 71a(1) of the PIL Act introduced legal uncertainty into the process of recognising foreign court decisions from a principle point of view. Namely, given that the PIL Act emphasises the need for legalisation exclusively in procedures for the recognition of a foreign court decision on adopting a child, ie when the country of origin of the decision is not a party to the international treaty regulating international adoption, *argumentum a contrario* points to the conclusion that for all other parties to court decisions whose recognition is carried out on the basis of the PIL Act, regardless of the legal matter, proof of legalisation in terms of the LPD Act does not have to be submitted. In particular, the question arises as to whether the provision of art 71a(1) of the PIL Act can be interpreted as a kind of derogation from the LPD Act in relation to all other foreign court decisions originating from countries with which the Republic of Croatia has not concluded a valid international treaty on the basis of which certification of foreign public documents, including court decisions, would be regulated in a different way. Thus, the provision of art 71a(1) of the PIL Act concerning the prescription of the obligation to legalise a foreign court decision on adoption caused a logical inconsistency between the provisions of the PIL Act and the LPD Act, which is against the requirement for the coherence of the legal system.²¹⁷ In terms of the use of foreign court decisions as public documents, impaired coherence of the domestic legal system applies equally to the procedures for deciding on recognition as the main matter and on recognition that is decided as a preliminary (prejudicial) issue. The aforementioned legislative intervention may also lead to the conclusion that by court decisions before the amendment of the PIL Act, the legislator renounced the status of public documents, both according to the *lex loci actus*, and secondarily according to the relevant Croatian law, so they did not even come within the scope of the provisions of the LPD Act. However, such an argument is not tenable. It should be taken into account that the Supreme Court of the Republic of Croatia, albeit from the criminal law level, took the position that court decisions are public documents.²¹⁸ Croatian substantive criminal law does not define an autonomous concept of public documents, while the criminal law doctrine reaches for normative determinations of public documents

217 Duško Vrbanić, *Država i pravo* (Golden marketing 2003) 425.

218 Supreme Court of the Republic of Croatia, judgment I Kž-904/05-8 of 13 June 2006.

in terms of the CPA and the GAP Act.²¹⁹ Thus, in any case, if the *lex loci actus* cannot be applied, at least from the aspect of Croatian law, (foreign) court decisions enjoy the status of public document.

As a result of the above, it should be assumed that in recognition procedures, regardless of the legal matter, foreign court decisions should continue to be subject to the provisions of the LPD Act, both in the application of the provision on the qualification of a foreign document as public, and consequently in legalisation, unless otherwise specified by international treaties. Namely, it is not logical for foreign court decisions to have legal effects in the Republic of Croatia after they have been recognised on the basis of the PIL Act, without having previously been subjected to the verification of the authenticity through the legalisation procedure, while on the other hand, within the meaning of art 231 of the CPA, foreign public documents that are intended to serve exclusively and solely as a means of proof would be subject to stricter control in terms of the verification of the authenticity in the legalisation procedure, unless otherwise specified by international or European law.²²⁰ In this sense, it is necessary to distinguish between the legal and evidentiary value of foreign public documents, including foreign court decisions. Foreign court decisions acquire their legal force by recognition, and in that case, they are equivalent in effect to decisions of domestic courts, while foreign court decisions acquire their evidentiary value after they have been duly certified (legalised), unless otherwise stipulated by international treaties or European law, and in that case, they are bound by the presumption of authenticity of the document, just like domestic public documents.²²¹ However, despite the presumption of authenticity of public documents as a formal rule of evidence within the meaning of the CPA, it should be kept in mind that it is possible to prove that a public document is false.²²² On the other hand, if a foreign court decision, as a public document, is used before the court as a means of proof, then its wording in a refutable manner proves exclusively that what was established or produced by it exists even after the moment to which its formality refers, and as a public document, it proves the content of the explanation as such, but not the authenticity of the claims stated in the explanation of the decision.²²³ The regularity of the wording or legal dispositions in a public document, including a court decision, cannot be refuted within the evidentiary proceeding, but the aforementioned can be refuted exclusively in accordance with the procedural rules of the proceeding within

219 See: Maja Munivrana Vajda, 'Krivotvorenje isprave' in Davor Derenčinović (ed), *Posebni dio kaznenog prava*, prvo izdanje (Pravni fakultet Sveučilišta u Zagrebu 2013) 225.

220 PIL Act, art 66(1).

221 Dika (n 4) 542.; CPA, arts 230 and 231; LPD Act, art 1.

222 CPA, art 230(3).

223 Dika (n 4) 532–533.

the framework of which the public document was issued.²²⁴ Moreover, it is very likely that a foreign public document, as a means of proof in the proceedings, will not be the only and exclusive evidence, therefore the court will not necessarily make a decision in the proceedings only on the basis of the rule on the presumption of authenticity of the public document as a formal rule of evidence, but also by evaluating other evidence separately and all the evidence together, but also based on the results of the entire proceeding.²²⁵ Consequently, it should be considered that the legal force of a certain document still has a higher degree of effectiveness than the evidentiary value, and this points to a reasonable conclusion that, as a result, all foreign court decisions in the recognition process based on the PIL Act should all the more be previously legalised in terms of the LPD Act, unless otherwise stipulated by international treaties.

Finally, it should be concluded that in addition to satisfying the then-current political needs, the legislative intervention, expressed through art 71a(1) of the PIL Act, clearly had the purpose to educate the addressees, ‘step by step’, how to act in connection with the proposal for the recognition of a foreign court decision on adoption, although the aforementioned was already regulated by the PIL Act and the LPD Act. The educational character of art 71a(1) of the PIL Act can also be inferred from the explanation of the Proposal of the Act Amending the Private International Law Act, which the Government of the Republic of Croatia, as an authorised proposer, submitted to the Croatian Parliament. Thus, the Government states that the goal of the proposed act is, *inter alia*, to ensure that in the recognition process, a foreign court decision on adoption is delivered to domestic courts legalised ‘*in accordance with existing regulations*’.²²⁶

5. Conclusion

In legal theory, issues related to the application of a public document issued by the authorised body of one country in order to exercise a right or fulfill an obligation in another country, have caused numerous dilemmas and have been the impetus for legislative interventions at the national and supranational level. The development of information and communication technologies and the digitalisation of national, European and international adjudication in civil matters require a review of the functionality of the existing legal framework and its application, which is the subject of discussion in this contribution.

²²⁴ Triva and Dika (n 1) 514.

²²⁵ CPA, art 8.

²²⁶ Proposal of the Act Amending the Private International Law Act, 2, <https://sabor.hr/sites/default/files/uploads/sabor/2023-05-19/135803/PZ_498.pdf> accessed 17 January 2024.

Unanswered questions related to the application of paper public documents are further complicated when an attempt is made to answer them in the context of the application of digitised public documents. Namely, the differences in the rules of national legal systems, such as the refusal to issue an Apostille on certified copies of public documents for the purpose of legal order protection due to frequent fraudulent practices with certified copies, can be an additional problem when it comes to dealing with electronic documents. Furthermore, the absence of uniform rules on the authenticity of an electronic public document, especially if the national system limits its time validity, gives rise to doubts as to the validity of the issued Apostille. In the context of the Republic of Croatia and the legal certainty of entities when presenting Croatian electronic public documents to the authorities of other countries, it would be opportune to propose, as the most optimal solution, that the Republic of Croatia joins the e-APP programme, and consequently consistently applies dualism regarding the addition of Apostilles, depending on the form of the public document. In this case, a paper (physical) Apostille should be attached to public documents that originally exist in a paper (physical) form, while an e-Apostille should be attached exclusively to electronic public documents.

Certain questions also arise regarding the status of court decisions as public documents in the regime of the Brussels I bis Regulation and the Brussels II ter Regulation. There is a fundamental doubt as to whether the wording '*documents ... issued under this Regulation*' refers to all types of documents, including judgments, or only to documents whose issuance is prescribed by the Regulation. In this regard, it is not entirely clear how the provisions of national procedural law should treat a court decision of another Member State if it were to be used exclusively as a means of proof. Should it necessarily have an Apostille? In the same way, with regard to asserting the objection *res judicata*, which is declared in the context of litigation before the court of a Member State that is different from the Member State of origin of the decision, will it be necessary for the decision to be accompanied by an adequate certificate in terms of the Brussels I bis Regulation and the Brussels II ter Regulation because the wording of the decision *res judicata* represents a legal disposition of the court and as such expresses a certain legal situation, not a fact, so it is not even a question of using the decision as a means of proof in the sense of the usual understanding?

It is precisely the criticism expressed regarding the *ad hoc* legislative intervention that amended the PIL Act in such a way that, *inter alia*, additional prerequisites are prescribed for the recognition of a foreign court decision on adopting a child from a country that is not a party to the international treaty governing international adoption, illustrates the difficulties in seeking solutions to these open questions. Therefore, this contribution is an incentive for their deeper consideration and search for comprehensive answers before formulating unequivocal conclusions and solutions.

Facial Recognition Technology in Esports? Youth Protection vs. Human Rights Risks

Tsubasa Shinohara *

Institute of Humanities and Social Sciences, University of Tsukuba
ORCID 0000-0002-2972-7460

DOI: 10.54103/milanoup.215.c457

Abstract

Esports (‘competitive video games’ or ‘electronic sports’) have rapidly developed. Currently, the esports industry is composed of many esports stakeholders and becomes one of the worldwide economic markets. Due to such rapid growth, however, the esports society has faced many problems, such as doping, match-fixing, physical and mental health issues, and sexual harassment against vulnerable esports players etc. In this situation, some states enact national legislation on video games to protect children against negative consequences, such as violent scenes, images of sexual expression, gaming addiction and disorders. National legislation has created an age limitation for children to play competitive video games. Despite this, children still have access to esports activities because their parents or other adult give them prohibited video games. Therefore, it is difficult for states to restrict children’s access to competitive video games. In this situation, this chapter considers whether esports society should use facial recognition technology to protect youth esports players. To answer this main question, this chapter will examine the following research questions: (1) How has facial recognition technology been used in esports society?; (2) What human rights risks can be identified due to the use of facial recognition technology?; and (3) How should the esports society strike a balance between youth protection in esports and human rights risks caused by the use of facial recognition technology? Through this research, it may clarify how esports publishers and esports event/league organisers may evaluate the impact on fundamental human rights by using facial recognition technology in the esports society.

* Assistant Professor, University of Tsukuba (Institute of Humanities and Social Sciences), Ibaraki, Japan, shinohara.tsubasa.gb@u.tsukuba.ac.jp; Human Rights Officer, Swiss Esports Federation, Bern, Switzerland, tsubasa.shinohara@sesf.ch.

Keywords

Facial Recognition Technology, Esports, Youth Protection, Human Rights Risks

1. Introduction

Esports (‘competitive video games’ or ‘electronic sports’) have rapidly developed. According to the Newzoo’s free report in 2022, the global revenue of the esports industry in 2021 reached 1,136.5 million dollars and the expected global revenue by 2025 will be 1,866.2 million dollars.¹ At the present time, the esports industry is composed of many esports stakeholders, such as esports publishers (eg Electronic Sports League (ESL), Valve and Riot Games), electronic equipment companies (eg Logitech and Dell), television and media companies (eg CBS, ESPN and Swisscom), streaming platform providers (eg Twitch and YouTube), video game distributors (eg Google Play Store and Apple Store) etc.² Thus, it can be said that the esports industry becomes one of the worldwide economic markets.

Due to such rapid growth, the esports society has faced many problems, such as doping,³ match-fixing,⁴ physical and mental health issues,⁵ sexual harassment against vulnerable esports players⁶ etc. In this situation, some states enact national legislation on video games to protect children against negative consequences, such as violent scenes, sexual expression images and gaming addiction

1 Newzoo, *Global Esports & Live Streaming Market Report 2022* (Free Version, 2022) at 34, <<https://newzoo.com/insights/trend-reports/newzoo-global-esports-live-streaming-market-report-2022-free-version/>> accessed 30 May 2024.

2 See Tsubasa Shinohara, ‘Global Governance in International Esports Society?’ (2023) 27(4) *Gaming Law Review* 1.

3 Tsubasa Shinohara, ‘The Protection of Esports Players against the Use of Doping Substances and Methods under the European Convention on Human Rights: The Swiss Example’ (2021) 1(1) *International Journal of Esports* 1 <<https://www.ijesports.org/article/69/html>> accessed 30 May 2024.

4 ‘The continued rise of eSport – Efforts to combat match fixing and improve integrity’ (*LawInSport*, 2 September 2016) <www.lawinsport.com/topics/features/item/the-continued-rise-of-esport-efforts-to-combat-match-fixing-and-improve-integrity> accessed 30 May 2024; Ryan P Toomey, ‘Upholding the Integrity of Esports To Successfully and Safely Legitimize Esports Wagering’ (2019) 23(1) *Gaming Law Review* 14–16; Peter K Czegledy, ‘Esports Integrity Policies’ (2021) 25(4) *Gaming Law Review*, 167; Atish Ghoshal, ‘Ethics in Esports’ (2019) 23(5) *Gaming Law Review* 340.

5 Tsubasa Shinohara, ‘The Protection of Professional Esports Players Against Physical and Mental Health Problems under the International Covenant on Economic, Social and Cultural Rights’ (2022) 13(1) *UNLV Gaming Law Journal* 1.

6 Jay Castello, ‘Foul play: tackling toxicity and abuse in online video games’ *The Guardian* (17 August 2018); John T Holden and others, ‘The #E-Too Movement: Fighting Back Against Sexual Harassment in Electronic Sports’ (2020) 52(1) *Arizona State Law Journal*, 11–14.

and disorders.⁷ The national legislation creates an age limitation for children to play competitive video games. Nevertheless, children can still have access to esports because their parents or other adults may give them prohibited video games.⁸ Therefore, it is difficult for states to restrict children's access to competitive video games.

In this connection, facial recognition technology has gradually become a part of our daily lives. For instance, Apple Inc. uses 'Face ID' to unlock iPhones, authorise purchases, and download apps without the need for passwords.⁹ At airports, facial scanning machines simplify the boarding process for passengers.¹⁰ In the context of esports, the technology has been used to restrict children's access to esports activities in order to protect them against gaming addiction.¹¹ For instance, the Chinese government has implemented a national

-
- 7 On 26 March 2021, the German Federal Council approved the reform of the Youth Protection Act submitted by the Federal Ministry of Family Affairs that restricts access of children to the internet in order to protect them against harmful contents, sexual exploitation and cyberbullying. This new law entered into force from 1 May 2021. *Zweites Gesetz zur Änderung des Jugendschutzgesetzes*, 9 April 2021, BGBl I 2021, N 16, 15 April 2021, S 742. See also 'Bundesrat billigt Reform des Jugendschutzgesetzes' (BMFSFJ, 26 March 2021) <www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/bundesrat-billigt-reform-des-jugendschutzgesetzes-161184> accessed 30 May 2024; 'Zweites Gesetz zur Änderung des Jugendschutzgesetzes', (BMFSFJ, 26 March 2021) <www.bmfsfj.de/bmfsfj/service/gesetze/zweites-gesetz-zur-aenderung-des-jugendschutzgesetzes-147956> accessed 30 May 2024.
 - 8 Joyce Cheng and Iris Zhao, 'Chinese internet giant introduces facial recognition technology in a bid to control underage gaming' *ABC News* (21 July 2021) <www.abc.net.au/news/2021-07-22/chinese-gaming-company-midnight-patrol-using-facial-recognition-/100306444> accessed 30 May 2024.
 - 9 'About Face ID advanced technology' (*Apple*, 10 January 2024) <<https://support.apple.com/en-us/HT208108>> accessed 30 May 2024. See also Lindsey Jacques, 'Facial Recognition Technology and Privacy: Race and Gender – How to Ensure the Right to Privacy is Protected' (2021) 23(1) *San Diego International Law Journal* 111, 116–117.
 - 10 Narita Airport in Japan started 'Face Express' to use facial recognition technology to facilitate boarding process <www.narita-airport.jp/html/faceexpress/en/index.html> accessed 30 May 2024; see also World Economic Forum, UNICRI, INTERPOL and Netherlands Police, 'A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations' (October 2021) 10 <www.weforum.org/whitepapers/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations/> accessed 30 May 2024.
 - 11 Tiffany May and Amy Chang Chien, 'Game Over: Chinese Company Deploys Facial Recognition to Limit Youth's Play' (*The New York Times*, 8 July 2021), <www.nytimes.com/2021/07/08/business/video-game-facial-recognition-tencent.html> accessed 30 May 2024; Sean Hollister, 'How Tencent's sweeping new facial scans will catch Chinese kids playing past curfew' (*The Verge*, 9 July 2021), <www.theverge.com/2021/7/9/22567029/tencent-china-facial-recognition-honor-of-kings-game-for-peace> accessed 30 May 2024; Hospes Coetu, 'Risks of Facial Recognition in Gaming' (*xsreviews*, 24 November 2020) <<https://xsreviews.co.uk/editorial/risks-of-facial-recognition-in-gaming/>> accessed 30 May 2024.

law prohibiting minors from playing video games between 10pm and 8am.¹² To enforce this law, it started ‘online patrol’ by using facial recognition technology to pick up young gamers.¹³ Therefore, if esports society may use this technology to protect young esports players, it might play an important role in the protection of young esports players against negative consequences due to esports activities. However, the use of facial recognition technology may cause human rights risks, particularly concerning the right to privacy, due to the collection and retention of sensitive personal data (ie biometric data).¹⁴

In this situation, this chapter will consider whether the esports society should use facial recognition technology to protect young esports players. To answer this main question, it will examine the following research questions: (1) How has facial recognition technology been used in esports society?; (2) What human rights risks can be identified due to the use of facial recognition technology?; and (3) How can the use of facial recognition technology be justified in esports activities? This research will serve to clarify how esports publishers and esports event/league organisers may assess an impact on fundamental human rights by using the facial recognition technology in the esports society.

In the light of the foregoing, this chapter will be divided into the following sections: After this introduction, it will provide an overview of how facial recognition technology is currently being used in the esports society to protect young esports players against negative consequences. Furthermore, it will examine the right to privacy guaranteed by international human rights law and identify human rights risks associated with the use of facial recognition technology. On this basis, this chapter will consider how the esports society should strike a balance between the protection of young esports players and the protection of their rights to privacy when it uses the facial recognition technology in esports. Finally, it will answer the main question of whether the esports society should use facial recognition technology to protect young esports players.

12 Javier C Hernández and Albee Zhang, ‘90 Minutes a Day, Until 10 P.M.: China Sets Rules for Young Gamers’ (*The New York Times*, 6 November 2019) <www.nytimes.com/2019/11/06/business/china-video-game-ban-young.html> accessed 30 May 2024.

13 Chandan Khanna, ‘China to impose curfew on young gamers in bid to cut gaming addiction rates’ (*ABC News*, 7 November 2019) <www.abc.net.au/news/2019-11-07/china-imposes-online-gaming-curfew-tackles-video-game-addiction/11680522> accessed 30 May 2024.

14 See Manon Laganà, ‘Facial Recognition And Human Rights In Europe’ (*Human Rights Pulse*, 1 April 2022) <www.humanrightspulse.com/mastercontentblog/facial-recognition-and-human-rights-in-europe> accessed 30 May 2024; Council of Europe, ‘Facial recognition: strict regulation is needed to prevent human rights violations’ (*Council of Europe*, 28 January 2021) <<https://www.coe.int/en/>> accessed 30 May 2024; Elizabeth Fernandez, ‘Facial Recognition Violates Human Rights, Court Rules’ (*Forbes*, 13 August 2020) <www.forbes.com/sites/fernandezelizabeth/2020/08/13/facial-recognition-violates-human-rights-court-rules/?sh=4823b4ca5d44> accessed 30 May 2024.

2. Facial recognition technology in esports?

As previously mentioned, China has implemented facial recognition technology to enforce its national law prohibiting young gamers from playing between 10pm and 8am, with the aim of protecting minors from gaming addiction. However, how should facial recognition technology be used in esports activities? To answer this question, this section will firstly provide an overview of what facial recognition technology is, and then describe how it is currently being used in the esports society.

2.1. What is facial recognition technology?

First of all, what is facial recognition technology? According to the Cambridge Online English Dictionary, the term ‘facial recognition’ means ‘technology that makes it possible for a computer to recognize a digital image of someone’s face’.¹⁵ More precisely, Elizabeth McClellan indicated that ‘[f]acial recognition technology is an algorithm used to recognize a human face through the use of biometrics, which track facial features from a photo or video’.¹⁶ Furthermore, the Danish Institute for Human Rights explained that:

Facial recognition is based on technology that captures biometric data to identify natural persons. The technology has many uses, ranging from comparing one image with one individual (so-called ‘one-to-one’ comparison) to more general surveillance of citizens and comparison of facial images against large databases (‘one-to-many’ comparison).¹⁷

Furthermore, it can be trained to improve the ability for the identification and verification of human faces via machine learning technology through the analysis of the large quantities of facial images.¹⁸ In other words, this technology is combined with machine learning technology to enhance their capacity and quality to recognise human faces and to identify a specific person through the analysis of large quantities of facial images. On this basis, this art defines the term ‘facial recognition technology’ as an algorithm used to recognise human

15 ‘Meaning of facial recognition in English’ (*Dictionary Cambridge*) <<https://dictionary.cambridge.org/dictionary/english/facial-recognition>> accessed 30 May 2024.

16 Elizabeth McClellan, ‘Facial Recognition Technology: Balancing the Benefits and Concerns’ (2020) 15(2) *Journal of Business & Technology Law* 363.

17 The Danish Institute for Human Rights, ‘Memo: Facial Recognition to Combat Crime’ (*The Danish Institute for Human Rights*, 20 February 2020) 3 <www.humanrights.dk/publications/facial-recognition-combat-crime> accessed 30 May 2024.

18 Sarah Chun, ‘Facial Recognition Technology: A Call for the Creation of A Framework Combining Government Regulation and A Commitment to Corporate Responsibility’ (2020) 21(4) *North Carolina Journal of Law & Technology* 99, 104–105.

faces and to identify and verify a specific person via machine learning through the analysis of a huge amount of facial images.

Based on this definition, what benefits can facial recognition technology provide us? This technology is used for the following three purposes¹⁹: (1) identification (identifying one person from among others in a database (one-to-many comparison)); (2) authentication/verification (verifying a person's identity, such as passport photos (one-to-one comparison)); and (3) classification/categorisation (classifying a facial image into sex, colour and age etc. (matching general characteristics)).²⁰ It would be beneficial for the esports society to utilise this technology to ensure a safe environment for young esports players. In doing so, esports publishers and esports event/league organisers need to verify the age of players using their facial images and personal information provided during registration. This method would prevent underage players from accessing esports activities.

2.2. Different reactions to the use of facial recognition technology in Asia and Europe

Based on this definition, this subsection will provide an overview of the different reactions to the use of facial recognition technology in Asian and European countries. This is because each country has taken a different approach to the use of facial recognition technology.²¹

19 See Vera Lúcia Raposo, 'Do not remember my face: uses of facial recognition technology in light of the general data protection regulation' (2022) *Information & Communications Technology Law* 45.

20 Christopher S Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy' (1999) 9(1) *Southern California Interdisciplinary Law Journal* 295, 306; Desara Dushi, 'The use of facial recognition technology in EU law enforcement: Fundamental rights implications' (*Global Campus Policy Briefs: South East Europe*, 2020) 3 <<http://dx.doi.org/10.25330/528>> accessed 30 May 2024; Laganà (n 14); FRA, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA, 21 November 2019) 7-8. <<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>>; Tambiama Madiega and Hendrik Mildebrath, *Regulating facial recognition in the EU* (European Parliament September 2021) 1–2.

21 Russian Federation has already used the facial recognition technology for surveillance of the Russian citizens. In this situation, victims submitted a complaint about a violation of their rights to respect for private life under art 8 of the European Convention on Human Rights (ECHR) against the Russian government before the European Court of Human Rights (ECtHR). See Anastasiia Kruope, 'Moscow's Use of Facial Recognition Technology Challenged Activists File an Application to European Court of Human Rights' (*Human Rights Watch*, 8 July 2020), <www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged> accessed 30 May 2024; Jacques (n 9) 137–138; regarding the United States, *ibid* 139–141; Elizabeth A Rowe, 'Regulating Facial Recognition Technology in the Private Sector' (2020) 24(1) *Stanford Technology Law Review* <<https://law.stanford.edu/publications/regulating-facial-recognition-technology-in-the-private-sector/>> accessed 30 May 2024.

In Asian countries, there is often less opposition to the deployment of machines with facial recognition technology. For instance, Japan decided to use facial recognition technology to check physical temperature and vaccination status.²² In South Korea, the government launched a pilot project to use facial recognition technology of CCTV cameras to track the movement of infected people with the COVID-19 in 2021.²³ Furthermore, China uses this technology to monitor every actions of Chinese citizens²⁴ and invented other facial recognition technology which is capable of identifying human faces wearing a mask.²⁵ In addition to this, the Chinese government enforces Chinese population to scan their faces before using mobile internet services.²⁶ India started to use the facial recognition technology in various locations to monitor the population during COVID-19, even though there was no national legislation in place to govern its use.²⁷ In light of these examples, Asian countries tend to face less opposition when deploying facial recognition technology.²⁸

-
- 22 Kyodo News, 'Japan firm NEC to introduce facial recognition vaccination check system' (*Kyodo News*, 3 December 2021) <<https://english.kyodonews.net/news/2021/12/45d-18baf8341-nec-to-introduce-facial-recognition-vaccination-check-system.html>> accessed 30 May 2024; Nick Statt, 'ACLU sues facial recognition firm Clearview AI, calling it a "nightmare scenario" for privacy' (*The Verge* 28 May 2020) <www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws> accessed 30 May 2024.
 - 23 Jin Yu Young, 'A South Korean city will test facial recognition as a way to track the virus' *The New York Times* (13 December 2021) <www.nytimes.com/2021/12/13/world/asia/south-korea-facial-recognition-coronavirus.html> accessed 30 May 2024.
 - 24 Chun (n 18) 109–111; Simon Denyer, 'Beijing bets on facial recognition in a big drive for total surveillance' *The Washington Post* (7 January 2018) <www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?tid=lk_interstitial_manual_13> accessed 30 May 2024.
 - 25 Seungha Lee, 'Coming into Focus: China's Facial Recognition Regulations' (*CSIS*, 4 May 2020), <www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations> accessed 30 May 2024.
 - 26 Rosie Perper, 'Chinese government forces people to scan their face before they can use internet as surveillance efforts mount' (*Business Insider*, 2 December 2019) <www.businessinsider.com/china-to-require-facial-id-for-internet-and-mobile-services-2019-10?r=US&IR=T> accessed 30 May 2024; Jane Li, 'Getting a new mobile number in China will involve a facial-recognition test' (*Quartz*, 3 October 2019) <<https://qz.com/1720832/china-introduces-facial-recognition-step-to-get-new-mobile-number>> accessed 30 May 2024.
 - 27 Konina Mandal, 'Facial Recognition Technology and its Impact on Privacy Rights of Children' (2021) 4(4) *International Journal of Law Management & Humanities* 1142, 1142–1144 ; Murali Krishnan, 'Facial recognition software spreads across India but regulation is slow' (*rfi*, 6 August 2022) <www.rfi.fr/en/international/20220806-facial-recognition-software-spreads-across-india-but-regulation-is-slow> accessed 30 May 2024.
 - 28 However, Chinese District Court decided that the use of facial recognition technology to enter into the zoo was an excessive interference with the right to privacy. See Eva Dou, 'China built the world's largest facial recognition system. Now, it's getting camera-shy' *The Washington Post* (30 July 2022) <www.washingtonpost.com/world/>

In contrast to the situations of Asian countries, the use of facial recognition technology has been recognised as a sensitive issue in Europe. In France and the United Kingdom, the law enforcement authorities, especially police, started to experiment the facial recognition technology to prevent terrorism.²⁹ However, the European Parliament recently called for a ban on the use of facial recognition technology in public space.³⁰ Although Germany strongly supports this position,³¹ France is not in favour of total ban on the use of facial recognition technology.³² The UK courts have already examined the use of facial recognition technology with CCTV camera by police in *R (on the application of Bridges) v Chief Constable of South Wales Police*.³³ In this case, the Court of Appeal considered that the use of facial recognition technology infringed the right to respect for private life under art 8(1) of the ECHR, but the interference by the South Wales Police Force (SWP) with the art 8(1)'s right could be justified

facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html> accessed 30 May 2024.

29 Monika Zalnieriute, 'Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State' (2021) 22(2) *Science and Technology Law Review* 284, 286-287.

30 Melissa Heikkilä, 'European Parliament calls for a ban on facial recognition' (*Politico*, 6 October 2021) <www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/> accessed 30 May 2024; Clothilde Goujard, 'Europe edges closer to a ban on facial recognition' (*Politico*, 20 September 2022) <www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/> accessed 30 May 2024.

31 Melissa Heikkilä, 'German coalition backs ban on facial recognition in public places' (*Politico*, 24 November 2021) <www.politico.eu/german-coalition-backs-ban-on-facial-recognition-in-public-places/> accessed 30 May 2024.

32 For instance, the Conseil d'État authorised the creation of Alicem ('Authentification en ligne certifiée sur mobile'). This service permits smartphone users with a passport or residence permit to identify themselves for access to online services. However, this service requires the users to register their facial images by means of facial recognition technology. See Décret n°2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé «Authentification en ligne certifiée sur mobile». Gérard Haas, 'Reconnaissance faciale: Alicem validée par le Conseil d'État' (*haas avocats*, 17 November 2020), <<https://info.haas-avocats.com/droit-digital/reconnaissance-faciale-alicem-validee-par-le-conseil-detat>> accessed 30 May 2024. Furthermore, French airports started to use facial recognition technology for identity checks, see Pierre Jova, 'La reconnaissance faciale débarque à l'aéroport' *La Croix* (9 July 2018) <www.la-croix.com/France/Securite/reconnaissance-faciale-debarque-l aeroport-2018-07-09-1200953660> accessed 30 May 2024.

33 *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, paras 1-3; Rafe Jennings, 'Facial Recognition Technology not "In Accordance with Law"' (*UK Human Rights Blog*, 13 August 2020) <<https://ukhumanrightsblog.com/2020/08/13/facial-recognition-technology-not-in-accordance-with-law/>> accessed 30 May 2024. Regarding the case summary, see Simons+Simons, 'UK Court of Appeal finds facial recognition technology unlawful' (*Simons+Simons*, 2 September 2020) <www.simmons-simmons.com/en/publications/ckelg1z7p8kjt09008l0bet7c/uk-court-of-appeal-finds-facial-recognition-technology-unlawful> accessed 30 May 2024. Regarding this case summary, see Monika Zalnieriute (n 29) 292-296.

under art 8(2) of the ECHR. However, it stated that the SWP's interference was not in accordance with the law³⁴ and the SWP did not conduct adequate 'data protection impact assessment' (DPIA).³⁵ Therefore, it decided that there was an infringement of art 8 of the ECHR because the SWP's interference did not satisfy the art 8(2)'s conditions.³⁶ Therefore, European countries are reluctant to accept the use of facial recognition technology in order to protect the right to respect for private life under art 8 of the ECHR.

In short, Asian countries generally did not face significant opposition to the use of facial recognition technology, while European countries (excluding France) have been strongly opposed to it. This is largely due to concerns that collecting facial images could infringe on the right to privacy, which will be discussed in the following subsection. Accordingly, different reactions of Asian and European countries to the use of facial recognition technology can be discerned.

2.3. Facial recognition technology in esports

In light of the different reactions of Asian and European countries to the use of facial recognition technology, this subsection will provide an overview of how the esports society uses facial recognition technology. In doing so, it will refer to some examples, in particular China and European countries.³⁷

As previously mentioned, China has implemented facial recognition technology to prevent gaming addiction and enforce its national law that prohibits minors from playing electronic games during 10 pm to 8 am. To enforce this law, the Chinese gaming company, Tencent Games, has introduced facial recognition technology to prevent minors from playing at night.³⁸ However, the majority of young esports players may still have access to competitive video games because their parents provide them with smartphones or gaming IDs for competitive video games.³⁹

34 *R (on the application of Bridges)* paras 54–130.

35 *ibid* paras 145–154.

36 *ibid* paras 209–210.

37 In South Korea, the government enacted the Youth Protection Act (or the Shutdown Law), Youth Protection Act, Act No 15987, 18 December 2018, prohibiting children under the age of 16 from playing online video games between 0:00 am to 6:00 am under art 26(1) of the Shutdown Law to protect young esports players against negative consequences in 2011. However, it was abolished by the National Assembly of the South Korea in 2021 to revise the Youth Protection Act. See Korea Herald, 'Shutdown law shuttered' (*The Korea Herald*, 16 November 2021) <www.koreaherald.com/view.php?ud=20211115000803> accessed 30 May 2024.

38 Niji Narayan, 'Tencent Introduces Face Recognition Feature to Prevent Children from Gaming at Night' (*European Gaming*, 13 July 2021) <<https://europeangaming.eu/portal/latest-news/2021/07/13/96109/tencent-introduces-face-recognition-feature-to-prevent-children-from-gaming-at-night/>> accessed 30 May 2024.

39 Cheng and Zhao (n 8).

European countries have not yet used facial recognition technology in the context of esports. In this connection, the European Parliament called for a ban on the use of facial recognition technology in public space.⁴⁰ In this sense, European countries are reluctant to use this technology to defend individuals' privacy in Europe. Therefore, esports publishers and event/league organisers in Europe are hesitant to use this technology and are subject to strict requirements under European data protection law.

To sum up, China is a leading country for the use of facial recognition technology in esports. European countries have faced huge obstacles to implement this technology in European esports activities because the use of this technology may cause a potential human right violation. In other words, it arbitrarily interferes with the right to privacy guaranteed by international human rights treaties. This issue has been recognised as one of the most concerning aspects for the use of the facial recognition technology.⁴¹ Therefore, the next section will consider if there is a violation of the right to privacy guaranteed by international human rights law.

3. Youth protection in esports vs. human rights risks caused by the use of facial recognition technology

Based on the previous section, it is clear that the esports society has gradually used the facial recognition technology. However, the following question may be raised: What human rights risks does the use of facial recognition technology cause? To answer this question, this section will examine the risk of a violation of the right to privacy (or the right to respect for private life) guaranteed by international human rights law, especially the Universal Declaration of Human Rights (UDHR),⁴² the International Covenant on Civil and Political Rights (ICCPR)⁴³ and the European Convention on Human Rights (ECHR).⁴⁴

40 Heikkilä (n 30); Goujard (n 30). Regarding this discussion, see Madiega and Mildebrath (n 20).

41 McClellan (n 16) 378–380.

42 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

43 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR). It is important to note that China does not ratify but signs the ICCPR so it has an obligation not to defeat the object and purpose of the ICCPR under Art 18(a) of the Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331 (VCLT). China acceded the VCLT on 3 September 1997.

44 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Children under 18 years old may also enjoy this protection under art 16 of the Convention on the Rights of the Child (CRC).⁴⁵

Under these human rights treaties, it is important to note that international human rights treaties impose on state parties the following two categories of legal obligations⁴⁶: (1) negative obligations to refrain from interfering with the enjoyment of rights; and (2) positive obligations to take necessary measures to prevent and protect human rights violations caused by states and non-state actors.⁴⁷ In the context of esports, esports publishers and esports event/league organisers are non-state actors and, thus, they are not held responsible for the implementation of both obligations under international human rights law. However, the state parties must implement positive obligations to prevent human rights violations caused by non-state actors.⁴⁸ Therefore, if esports publishers and esports event/league organisers infringe the right to privacy due to the use of the facial recognition technology, states must take necessary measures to avoid such human rights violations within the territories.⁴⁹

In light of the foregoing, this section will be divided into the following subsections: Firstly, it will consider if there is a violation of the right to privacy due to the use of facial recognition technology in light of the provisions of the ICCPR and ECHR.⁵⁰ If so, it will then take into consideration how the state interference can be justified to use this technology under these treaties.

3.1. Is there a violation of the right to privacy due to the use of facial recognition technology?

At the beginning of this section, this subsection will refer to art 12 of the UDHR, which reads as follow:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

45 Convention on the Rights of the Child, (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC). China signed and ratified the CRC.

46 See art 2(1) of the ICCPR; art 1 of the ECHR. See also OHCHR, 'The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) A/HRC/48/31 para 10.

47 Walter Kälin and Jörg Künzli, *The Law of International Human Rights Protection* (2nd edn, Oxford University Press, 2019) 87–90.

48 See *K.H. and Others v Slovakia*, App no 32881/04 (ECtHR, 28 April 2009) paras 44–48.

49 The use of facial recognition technology causes a violation of the right to human dignity, but this art will not consider this issue. See FRA (n 20) 20–21.

50 This article will not consider the provisions of the CRC.

In other words, this provision firstly guarantees the right to privacy for everyone at the international level. However, it is important to note that the UDHR has no legally-binding effect on states, but this non-legally binding norm was converted into a legal obligation after the adoption of the ICCPR in 1966.⁵¹ Therefore, this subsection will provide an overview of the right to privacy in the context of the use of facial recognition technology in light of art 17(1) of the ICCPR and art 8(1) of the ECHR.⁵² Furthermore, it will consider how the General Data Protection Regulation (GDPR)⁵³ may apply to the use of facial recognition technology in the context of esports because the GDPR is an important instrument for the protection of the right to privacy in Europe.

3.1.1 *The right to privacy under art 17 of the ICCPR*

First of all, art 17(1) of the ICCPR stipulates that ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation’. This provision guarantees the right to privacy which ‘is an expression of human dignity and is linked to the protection of human autonomy and personal identity’.⁵⁴ Under this provision, state parties to the ICCPR shall enact the national legislation prohibiting arbitrary or unlawful interference with individual’s privacy by state and non-state actors (positive obligations).⁵⁵

Regarding the protection of personal data, the Human Rights Committee (HRC)’s General Comment No 16⁵⁶ explains that ‘The gathering and holding of personal information on computers, data banks and other devices whether by public authorities or private individuals or bodies, must be regulated by law. (...)’.⁵⁷ In particular, it uses the term ‘other devices’ in this paragraph and this term should be interpreted to include the facial recognition technology on the basis of a *living document* doctrine which reflects the social and technological

51 Kälin and Künzli (n 50) 36.

52 The use of facial recognition technology also causes discrimination based on race, skin colour and gender. In this regard, see Jacques (n 9) 119–122; Joy Liddicoat, *Human Rights and the Internet* (Intersentia, 2021) 148.

53 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L119/1. In practice, this website is much easier to see the legal text of the GDPR: <<https://gdpr-info.eu>> accessed 30 May 2024.

54 OHCHR (n 46) para 7.

55 UN Human Rights Committee, ‘CCPR General Comment No. 16: Art 17 (The right to respect of privacy, family, home and correspondence and protection of honour and reputation)’ (8 April 1988) <www.refworld.org/legal/general/hrc/1988/en/27539> accessed 30 May 2024; Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (3rd edn, OUP, 2013) 541.

56 Art 28 ICCPR.

57 UN Human Rights Committee (n 55).

development for the interpretation of human rights treaties.⁵⁸ As had been mentioned in the previous section, the facial recognition technology has been grown up in our society and it cannot be ignored. In this situation, the OHCHR's Report on the Right to Privacy in the Digital Age (hereinafter: the OHCHR report) indicates:

Aspects of privacy that are of particular importance in the context of the use of AI include informational privacy covering information that exists or can be derived about a person and her or his life and the decisions based on that information, and the freedom to make decisions about one's identity.⁵⁹

Therefore, the right to privacy should be taken into account when the facial recognition technology with machine learning is used.

In conclusion, it can be considered that the use of facial recognition technology falls within the scope of art 17(1) of the ICCPR and the state parties are held responsible for taking necessary measures to protect personal information collected by the facial recognition technology. However, each state has no specific national legislation on the use of facial recognition technology. In this situation, how can the state parties implement the positive obligations to prevent a violation of the right to privacy against the use of facial recognition technology under art 17(1) of the ICCPR? In doing so, this art should refer to each national data protection law regulating the treatment of personal information by electronic device, but it cannot all be dealt with. Therefore, it will refer to the GDPR as an example to know how the personal data collected by the facial recognition technology should be treated and protected.

3.1.2. *The right to respect for private life under art 8 of the ECHR*

Furthermore, art 8(1) of the ECHR prescribes that 'Everyone has the right to respect for his private and family life, his home and his correspondence'. The ECtHR explains that the concept of 'private life' is a broad term covering the physical and psychological integrity of a person, an individual's physical and social identity, a right to personal development, and the right to establish and develop relationships with other human beings and the outside world.⁶⁰ On this basis, this provision imposes on state parties negative obligations to refrain from interference with private and family life and positive obligations to protect individuals from violations of their rights to private life.⁶¹ In particular, state

58 See David Harris and others, *Harris, O'Boyle & Warbrick: Law of The European Convention on Human Rights* (4th edn, OUP, 2018) 501.

59 OHCHR (n 46) para 7.

60 *Pretty v The United Kingdom*, App no 2346/02 (ECtHR, 29 April 2002) para 61; William A Schabas, *The European Convention on Human Rights: A Commentary* (Oxford University Press, 2015) 370.

61 *ibid* 367–369; Harris (n 58) 510–513.

parties must take legislative or administrative measures to implement negative obligations, but they may enjoy a certain margin of appreciation allowing them to decide how to strike a balance between the competing public and private interests or Convention rights.⁶²

Regarding the protection of personal data, David Harris and others point out that '[t]he collection, storage, and disclosure of information by the state about an individual will interfere with his right to respect for private life'.⁶³ Thus, the use of new technologies to collect biometric data may interfere with art 8(1)'s rights.⁶⁴ In this context, it can be interpreted that the use of facial recognition technology falls within the scope of art 8(1) of the ECHR on the basis of a living instrument doctrine.⁶⁵

In conclusion, the use of facial recognition technology is considered the interference with the right to respect for private life under art 8(1) of the ECHR because this technology can collect biometric data, especially facial images, by means of automated processing.⁶⁶

3.1.3 Data protection under the General Data Protection Regulation

Finally, this part will refer to the provisions of the GDPR in the context of the use of facial recognition technology as one of the examples of data protection law. As has been mentioned in the previous section, the facial recognition technology can collect sensitive personal data, especially biometric data,⁶⁷ without any explicit consent by data subjects.⁶⁸ In this regard, art 4(14) of the GDPR provides that:

'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person,

62 Schabas (n 60) 368; ECtHR, Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence (Council of Europe/European Court of Human Rights, Updated on 9 April 2024) para 8 <<https://ks.echr.coe.int/web/echr-ks/all-case-law-guides>> accessed 30 May 2024.

63 Harris (n 58) 538.

64 The retention of fingerprints, cellular samples and DNA profiles, which fall within the scope of the biometric data, by public authorities constitutes an interference with the right to respect for private life. *S and Marper v The United Kingdom*, App no 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 77 and para 86. See also *Peck v The United Kingdom*, App no 44647/98 (ECtHR, 28 January 2003) para 59; *Gaughran v The United Kingdom*, App no 45245/15 (ECtHR, 13 February 2020) para 63; ECtHR, Guide to the Case-Law of the of the European Court of Human Rights: Data Protection (Council of Europe/European Court of Human Rights, Updated on 29 February 2024) paras 24–30, <<https://ks.echr.coe.int/web/echr-ks/all-case-law-guides>> accessed 30 May 2024.

65 *ibid* paras 62 and 378.

66 Laganà (n 14).

67 Jacques (n 9) 114.

68 See R (*on the application of Bridges*) paras 21–23.

such as facial images or dactyloscopic data.⁶⁹

Furthermore, the Court of Justice of the European Union and the ECtHR has also recognised facial images as sensitive personal data (or biometric data).⁷⁰ Therefore, facial images collected by facial recognition technology can be categorised as ‘biometric data’.⁷¹

On this basis, art 5 of the GDPR stipulates that the processing of biometric data collected by facial recognition technology must be lawful, fair and transparent with an explicit consent and purpose.⁷² Regarding the explicit consent, arts 6(1)(a) and 7 of the GDPR stipulate that data subjects must give an explicit consent to data controllers and data processors to conduct a treatment of their personal data. If there is no explicit consent, the processing of special categories of personal data is prohibited under art 9(1) of the GDPR. However, the processing of biometric data can be justified if the data subjects give data controllers an explicit consent to process their personal data under art 9(2)(a) of the GDPR or this processing is necessary for the protection of other interests set forth in art 9(2)(b) to (j) of the GDPR. However, it is important to note that the GDPR has no legally-binding effect on non-member states to the Council of Europe.

In light of these provisions of the GDPR, when esports publishers and esports event/organisers use the facial recognition technology, data subjects (ie young esports players) have no opportunity to give an explicit consent to data controllers and processors (ie esports publishers and esports event/organisers) in order to process their biometric data because this technology automatically collect and process their personal data. Thus, the use of facial recognition technology can be recognised as the interference with the rights to privacy or the right to respect for private life.⁷³

3.2. Justification of interference with the right to privacy

Despite the fact that there is a violation of the right to privacy or the right to respect for private life due to the use of facial recognition technology,

69 See also art 3(13) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

70 Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670 paras 48-50; *Szabó and Vissy v Hungary*, App no 37138/14 (ECtHR, 12 January 2016) paras 52-89.

71 See also Madiega and Mildebrath (n 20).

72 *ibid* 11-14; FRA (n 20) 23-25.

73 The Danish Institute for Human Rights (n 17).

international human rights treaties make an exception for this protection.⁷⁴ In this regard, art 8(2) of the ECHR stipulates that:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In other words, the state interference with the right to respect for private life can be justified⁷⁵ only if it is in accordance with the law,⁷⁶ pursues a legitimate aim,⁷⁷ and is necessary in a democratic society.⁷⁸ To consider the necessity in a democratic society, the ECtHR considers the reason of state intervention is relevant and sufficient and the measures are proportionate to achieve the legitimate aim.⁷⁹ In doing so, the ECtHR examines that “a margin of appreciation should be left to the competent national authorities in striking a fair balance between the relevant conflicting public and private interests”.⁸⁰ If these conditions are satisfied, the state interference can be justified and, thus, there is no violation of art 8(1) of the ECHR.

In contrast to this, does the ICCPR prescribe the conditions for justifying the state interference with the right to privacy? For this question, the ICCPR does not specify the conditions for the restriction on the right to privacy, but art 17(1) of the ICCPR provides that any interference with the right to privacy must not be arbitrary or unlawful. In this regard, the OHCHR’s report explains the term ‘unlawful’ in the following meaning:

States may interfere with the right to privacy only on the basis of law and in accordance with that law. The law itself must comply with the provisions, aims and objectives of the International Covenant on Civil and Political Rights and must specify in detail the precise circumstances in which such interference is permissible.⁸¹

Furthermore, it also indicates the purpose of the term ‘arbitrary’ to “guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant, and should, in any event, be

74 Dushi (n 20) 5–8; see also OHCHR (n 46) paras 12–14.

75 Schabas (n 60) 401–406.

76 ECtHR (n 62) paras 15–21.

77 *ibid* paras 22–28.

78 *ibid* paras 29–31.

79 *Peck v The United Kingdom* para 76.

80 *ibid* para 77.

81 OHCHR (n 46) para 8.

reasonable in the particular circumstances”⁸². In other words, any interference with the right to privacy under art 17(1) of the ICCPR must be restricted under the conditions that such interference is provided by law, is necessary to achieve a legitimate purpose, and be proportionate to that purpose.⁸³ Accordingly, the right to privacy under art 17(1) of the ICCPR can be limited only when states parties to the ICCPR may prove that such interference is arbitrary or unlawful because it has no legitimate purpose, is not necessary for achieving such purpose and does not meet the proportionality requirement. Exceptionally, state parties may also derogate from art 17(1)’s obligations under the state emergency in accordance with art 4(1) of the ICCPR,⁸⁴ but this provision should not be examined in the context of esports.

In conclusion, restriction on the right to privacy (art 17(1) of the ICCPR) and the right to respect for private life (art 8(1) of the ECHR) can be justified only when such interference is provided by law, is necessary in a democratic society, and be proportionate to achieve that purpose.⁸⁵

4. How can the use of facial recognition technology be justified in esports activities?

Based on this understanding, how can the use of facial recognition technology be justified in esports activities? In doing so, it is necessary to strike a balance between youth protection in esports and human rights risks, that is an infringement of the right to privacy, caused by the use of facial recognition technology. However, international human rights law allows state parties to enjoy the margin of appreciation to choose the means for achieving the legitimate aim of state interference with human rights. Therefore, each state may decide if they should establish national legislation on the use of facial recognition technology. Furthermore, it is important to note that esports publishers and esports event/league organisers are not states but business enterprises and, thus, international human rights law cannot impose on them any legal obligations to protect the right to privacy guaranteed by art 17(1) of the ICCPR and art 8(1) of the ECHR. However, international human rights law imposes on state parties a positive obligation to ensure that even business enterprises should respect the provisions of international human rights treaties within their jurisdiction. In this context, the esports publishers and esports event/league organisers are also held responsible for the respect of human rights and should pay attention

⁸² *ibid* paras 8 and 39.

⁸³ *ibid* para 8.

⁸⁴ See UN Human Rights Committee, ‘General Comment no. 29, States of emergency (article 4) : International Covenant on Civil and Political Rights’ (31 August 2001) CCPR/C/21/Rev.1/Add.11.

⁸⁵ See also art 29(2) of the UDHR.

to use the facial recognition technology while preventing a potential violation of the right to privacy.

In light of the foregoing, this section will firstly overview a corporate responsibility to respect human rights under the United Nations Guiding Principles on Business and Human Rights (UNGPs)⁸⁶ because esports publishers and esports event/league organisers are not states actors, but business enterprises and, thus, they have no legal obligations under international human rights law. On this basis, it will then consider how the use of this technology can be justified in the context of esports in accordance with the human rights law and data protection law. More importantly, it will examine how the esports society should strike a balance between community's interests (ie youth protection against negative consequences (ie, gaming addiction and disorder)) and individual's interests (ie violation of the right to privacy) due to the use of facial recognition technology in esports.

4.1. The Responsibility of Business Enterprises to Respect Human Rights Under the UNGPs

As had been mentioned above, esports publishers and esports event/league organisers are business enterprises and, thus, international human rights law cannot impose legal obligations on them. However, the UNGPs, which is not legally-binding instrument, clarify a corporate responsibility for business enterprises to respect internationally recognised human rights. Principle 11 of the UNGPs stipulates that 'Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved'.⁸⁷

In this regard, the OHCHR reports states that this responsibility is considered 'human rights due diligence' "to identify, assess, prevent and mitigate adverse impacts on human rights that an entity may cause or to which it may contribute or be directly linked".⁸⁸ More precisely, Principle 13 of the UNGPs provides that:

The responsibility to respect human rights requires that business enterprises:

Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;

Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if

⁸⁶ OHCHR, *The UN Guiding Principles on Business and Human Rights implementing the United Nations 'Protect, Respect and Remedy' Framework* (United Nations, 2011).

⁸⁷ See also OHCHR (n 46) para 11.

⁸⁸ *ibid* paras 48–49.

they have not contributed to those impacts.

In the context of esports, esports publishers and esports event/league organisers have a negative responsibility to avoid infringing human rights law and a positive responsibility to address adverse human rights impacts through their esports activities in light of international human rights treaties (see Principle 12 of the UNGPs) when they deploy and operate the facial recognition technology in esports activities.⁸⁹

4.2. Justification of the Use of Facial Recognition Technology in Esports: Youth Protection Against Negative Consequences or Protection of the Right to Privacy?

The use of facial recognition technology constitutes an interference with the right to privacy or the right to respect for private life under international human rights treaties. So, the question is how it can be justified in the context of esports in order to protect young esports players against negative consequences, such as gaming addiction and disorders, caused by esports activities. In doing so, this subsection will consider how the esports publishers and esports event/league organisers should strike a balance between public and private interests in esports activities.

In this situation, public interests mean the protection of young esports players against negative consequences caused by esports activities. In particular, China has already been faced with gaming addiction and gaming disorder and, thus, it adopted national legislation prohibiting young esports players from playing from 10pm to 8pm. During this period, the public authority has conducted a night policing to enforce the implementation of this national legislation. In contrast to this, private interests can be considered the protection of the right to privacy due to the use of facial recognition technology. Based on this understanding, this chapter will consider how states or esports publishers and esports event/league organisers can justify the use of facial recognition technology to prevent negative consequences due to esports activities.

In light of the foregoing, states should enact a specific legislation on the use of facial recognition technology to achieve the prevention of negative consequences of young esports players. As had been mentioned in the previous subsection, however, they enjoy the margin of appreciation to decide if the use of this technology is permitted or not in light of the domestic situation. In contrast to this, esports publishers and esports event/league organisers should establish certain conditions for the use of the facial recognition technology to avoid an infringement of the right to privacy in accordance with international

⁸⁹ *ibid* para 48.

human rights law and data protection law.⁹⁰ Therefore, this subsection suggests the following minimum conditions for the use of the facial recognition technology in esports activities:

1. Esports publishers and esports event/organisers should determine and specify the purposes and methods of collecting sensitive personal data of young esports players by the facial recognition technology;
2. Esports publishers and esports event/organisers should clarify how and why the sensitive personal data of young esports players should be processed by the facial recognition technology;
3. Esports publishers and esports event/organisers should ensure that young esports players and their parent freely give them explicit consents to process their sensitive personal data by the facial recognition technology; and
4. Esports publishers and esports event/organisers should conduct a Data Protection Impact Assessment (DPIA)⁹¹ to identify potential risks arising out of the processing of sensitive personal data with the facial recognition technology and to minimise these risks as far as possible.⁹²

If all the conditions are satisfied, the use of facial recognition technology can be justified. In this situation, the esports society may use the facial recognition technology to protect young esports players against negative consequences in esports when it takes measures to mitigate human rights risks for a violation of the right to privacy under international human rights law.

5. Conclusion

This final section will answer the main question of whether esports society should use facial recognition technology to protect youth esports players? To answer this main question, this chapter examined the following research questions: (1) How has facial recognition technology been used in the esports society?; (2) What human rights risks can be identified due to the use of facial recognition technology?; and (3) How can the use of facial recognition technology be justified in esports activities? So, this chapter will address these research questions and then answer the main question posed in this chapter.

⁹⁰ Raposo (n 19) 19.

⁹¹ Regarding the DPIA, see Ben Welford, 'Data Protection Impact Assessment (DPIA)' (GDPR.EU) <<https://gdpr.eu/>> accessed 30 May 2024.

⁹² See Council of Europe, Commissioner for Human Rights, 'Unboxing artificial intelligence: 10 steps to protect human rights' (*Council of Europe*, May 2019) 7–8 <www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights> accessed 30 May 2024; Michael O'Flaherty, 'Opinion: Facial Recognition Technology and Fundamental Rights' (2020) 6(2) *European Data Protection Law Review* 173.

Firstly, how has facial recognition technology been used in the esports society? For this question, this chapter defined the term ‘facial recognition technology’ as an algorithm used to recognise human faces and to identify and verify a specific person via machine learning through the analysis of a huge amount of facial images. Based on this definition, this technology has been used for the prevention of crime by police in Asian countries. In the context of esports, China only uses it for the effective enforcement of Chinese law prohibiting minors from playing electronic games during 10pm to 8am. The purpose of this legislation is to protect young esports players against gaming addiction and disorder. Therefore, the esports society has already used the facial recognition technology to achieve youth protection in esports.

Based on this understanding, the second question in this chapter was what human rights risks can be identified due to the use of facial recognition technology. In this regard, it has been considered that the use of facial recognition technology causes a clear interference with the right to privacy guaranteed by art 12 of the UDHR, art 17(1) of the ICCPR, art 8(1) of the ECHR. However, state parties to these international human rights treaties may justify the use of facial recognition technology if it is prescribed by law and necessary for democratic society to achieve a legitimate aim. If these conditions are satisfied, the right to privacy can be restricted for the purpose of the use of facial recognition technology.

Finally, this chapter considered how the use of facial recognition technology can be justified in esports activities? Each state must take legislative measure to ensure the enjoyment of the right to privacy under art 17(1) of the ICCPR and art 8(2) of the ECHR. However, they may exercise the margin of appreciation to decide how they enact national legislation on the use of facial recognition technology. In this situation, the Pillar II of the UNGPs stipulates that business enterprises have a corporate responsibility to respect human rights. In doing so, it should take action to avoid a violation of the right to privacy caused by the use of the facial recognition technology and conduct a human rights impact assessment to mitigate the human rights risks.

In light of the foregoing, this chapter considered how the esports publishers and esports event/league organisers should strike a balance between public and private interests in esports activities. While public interests mean the protection of young esports players against negative consequences caused by esports activities, private interests can be considered the protection of the right to privacy due to the use of facial recognition technology. Based on this understanding, this chapter examined how states or esports publishers and esports event/league organisers can justify the use of facial recognition technology to prevent negative consequences due to esports activities. To achieve the prevention of negative consequences of young esports players, states should enact a specific legislation on the use of facial recognition technology, but they may exercise

the margin of appreciation under international human rights law. However, esports publishers and esports event/league organisers should establish certain conditions for the use of the facial recognition technology to avoid an infringement of the right to privacy in accordance with international human rights law and data protection law. Therefore, this chapter proposed several minimum conditions for the use of the facial recognition technology in esports activities in the previous section. If all the conditions are satisfied, it can be considered that the use of facial recognition technology may be justified. In this situation, the esports society can use the facial recognition technology for the purpose of protecting young esports players against negative consequences in esports when it takes measures to mitigate human rights risks for a violation of the right to privacy under international human rights law.

In conclusion, the esports society should use facial recognition technology to protect young esports players against negative consequences because this technology is helpful and useful for esports publishers and esports events/leagues organisers to verify if esports players meet the required age to have access to the esports activities. However, it is important to note that the esports society should strike a balance between the interests of youth protection and human rights concerns about the right to privacy guaranteed by art 12 of the UDHR, art 17(1) of the ICCPR and art 8(1) of the ECHR. If the esports society would like to use this technology, it must carefully pay attention to comply with data protection law because of the margin of appreciation of state parties to the international human rights treaties. If so, it can be considered that the use of facial recognition is permitted to be used by the esports publishers and esports event/league organisers to ensure a safe esports environment for young esports players.

Clinical Risk in Cross-Border eHealth

Cristina Campiglio

University of Pavia, Italy

ORCID 0000-0002-6748-5861

DOI: 10.54103/milanoup.215.c458

Abstract

Telemedicine and eHealth services raise a wide range of complex substantive legal issues. These complexities are further exacerbated by the ever-changing shape of the digital environment, last but not least in the light of the rapid spread of AI-based systems and related technologies. The challenging regulatory choices needed to adequately cope with the digital transformation of the healthcare sector become tremendously more pronounced when the provision of healthcare services based on ICTs bridges national borders. The contribution aims to identify solutions to possible conflicts of jurisdictions and laws within the European judicial area.

Keywords

eHealth, Telemedicine, Product Liability, Health Professional's Liability, Conflict of Jurisdiction, Conflict of Laws

1. eHealth and mHealth

The 2020-2025 Global Strategy delivered by the World Health Organization (WHO) acknowledges that 'digital transformation of health care can be disruptive; however, technologies such as the Internet of things, virtual care, remote monitoring, artificial intelligence, big data analytics, blockchain, smart wearables, platforms, tools enabling data exchange and storage and tools enabling remote data capture and the exchange of data and sharing of relevant information across the health ecosystem creating a continuum of care have proven potential to enhance health outcomes by improving medical diagnosis, data-based treatment decisions, digital therapeutics, clinical trials, self-management of care

and person-centred care as well as creating more evidence-based knowledge, skills and competence for professionals to support health care'.¹

Already the Digital Agenda for Europe presented in 2010 by the European Commission indeed has alluded to the potential of the Internet – that is 'borderless' – and of the 'innovative and advanced online services – such as (...) eHealth', hoping 'to achieve by 2020 widespread deployment of telemedicine services'.² The Digital Agenda for Europe envisages specific actions relating to eHealth with the view of achieving widespread deployment of patients' access to their health data and of enhancing interoperability between Information and Communication Technologies (ICTs) products and services. Taking the view that 'the deployment of eHealth technologies in Europe can improve the quality of care, reduce medical costs and foster independent living, including in remote places',³ the Commission indeed deplores that European citizens do not fully benefit from cross-border healthcare and eHealth technology.⁴

A year later the European Union (EU) legislator adopted the European Parliament and Council Directive 2011/24/EU of 9 March 2011 on the application of patients' rights in the field of cross-border healthcare⁵ (hereinafter the 'Directive on cross-border healthcare'). On one hand, the Directive implements the case law of the European Court of Justice (ECJ) on the EU citizens' right to reimbursement of costs of healthcare incurred in Member States other than that of the citizens' habitual residence,⁶ by extending the scope of that case

1 World Health Organization, 'Global strategy on digital health 2020-2025' [2021], CC BY-NC-SA 3.0. The Global Strategy also notes that 'there is a growing consensus in the global health community that the strategic and innovative use of digital and cutting-edge information and communications technologies will be an essential enabling factor towards ensuring that 1 billion more people benefit from universal health coverage, that 1 billion more people are better protected from health emergencies, and that 1 billion more people enjoy better health and well-being'. Always in 2021 the WHO published a set of guidelines on the ethical and regulatory implications of artificial intelligence applied to the healthcare sector; World Health Organization, 'Ethics and governance of artificial intelligence for health: WHO guidance' [2021], CC BY-NC-SA 3.0. Digital health is fully part of the Third Sustainable Development Goal of the United Nations Agenda 2030, which aims to ensure health and well-being to everyone, at all stages of life; UNGA Res 70/1 (21 October 2015) Un Doc A/RES/70/1.

2 Commission, 'A Digital Agenda for Europe' (Communication) COM (2010) 245 final.

3 *ibid* 29.

4 Commission, 'EU Citizenship Report 2010 – Dismantling the obstacles to EU citizens' rights' (Communication) COM (2010) 603 final, 8–9.

5 [2011] OJ L 88/45.

6 *eg* Case C-255/09 *Commission v Portugal* [2011] ECR I-10547. The ECJ case law is aptly summarized in the Directive's preamble. In particular, recital n 11 reads that: 'This Directive should apply to individual patients who decide to seek healthcare in a Member State other than the Member State of affiliation. As confirmed by the Court of Justice, neither its special nature nor the way in which it is organised or financed removes healthcare from the ambit of the fundamental principle of the freedom to provide services. However, the Member State of affiliation may choose to limit the reimbursement of cross-border healthcare for reasons

law as to encompass healthcare provided through eHealth and telemedicine⁷. On the other hand, it provides for the creation of ‘a voluntary network linking national authorities responsible for eHealth designated by the Member States’. The objectives of this network are to: ‘(a) work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare; (b) develop guidelines on: (i) a non-exhaustive list of data that are to be included in patients’ summaries and that can be shared between healthcare professionals to enable continuity of care and patient safety across borders; and (ii) effective methods for enabling the use of medical information for public health and research; (c) support Member States in developing common identification and authentication measures to facilitate the transferability of data in cross-border healthcare’ (art 14).⁸

In 2018 the European Commission published a Communication on the digital transformation of health and care.⁹ The Communication identifies three areas of priority for future EU’s actions: a) citizens’ secure access to their health data, including across borders; 2) personalised medicine through shared European data infrastructure; 3) citizen empowerment with digital tools for user feedback and person-centred care.¹⁰ Overall, the European Commission has stressed the wide-ranging beneficial impact that digital technologies, such as 5G mobile communication, Artificial Intelligence (AI) and supercomputing, may exert in increasing the well-being of EU citizens, in fostering innovation of the health sector and scientific research.¹¹

relating to the quality and safety of the healthcare provided, where this can be justified by overriding reasons of general interest relating to public health. The Member State of affiliation may also take further measures on other grounds where this can be justified by such overriding reasons of general interest. Indeed, the Court of Justice has laid down that public health protection is among the overriding reasons of general interest that can justify restrictions to the freedom of movement envisaged in the Treaties’.

7 Recital n 26 reads that: ‘The Court of Justice has held that the Treaty provisions on the freedom to provide services include the freedom for the recipients of healthcare, including persons in need of medical treatment, to go to another Member State in order to receive it there. The same should apply to recipients of healthcare seeking to receive healthcare provided in another Member State through other means, for example through eHealth services.’

8 Art 14(2) last sentence ‘(...) The objectives referred to in points (b) and (c) shall be pursued in due observance of the principles of data protection as set out, in particular, in Directives 95/46/EC and 2002/58/EC. (...) The Commission shall, in accordance with the regulatory procedure referred to in art 16(2), adopt the necessary measures for the establishment, management and transparent functioning of this network.’

9 Commission, ‘Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society’ (Communication) COM (2018) 233 final.

10 *ibid* 3–13.

11 *ibid* 1–3.

Nowadays the concept of ‘eHealth’ is used to broadly denote tools and services that rely on Information and Communication Technologies (ICTs) to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health. More specifically, the notion encompasses a wide range of services and information technology such as information systems and Electronic Health Records (EHR), Electronic Health Platforms (EHP), electronic transmission of prescriptions or referrals (e-prescription, e-referrals), evidence-based medicine, consumer health informatics, online pharmacy and telemedicine. A particular form of medical and public health practice supported by mobile devices such as phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices, is also rapidly spreading.¹² This practice of ‘mobile healthcare’ (‘mHealth’) includes applications that may connect to medical devices or sensors (bracelets or watches), health information/medication reminders provided by text (sms) and telemedicine provided wirelessly. AI-driven applications that encompass genuine medical services, requiring a health professional for diagnosis and/or treatment, fall within the concept of ‘e-Health’: not so mere self-control/wellbeing applications.

2. Cross-border telemedicine

‘Telemedicine’ refers to ‘the provision of healthcare services, through the use of ICTs, in situations where the health professional¹³ and the patient (or two health professionals) are not in the same location. It involves secure

12 See Commission, ‘Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps. Accompanying the document Green Paper on mobile Health (“mHealth”)’ (Staff Working Document) SWD (2014) 135 final; Commission, ‘Green Paper on mobile Health (“mHealth”)’ (Communication) COM (2014) 219 final, para 3.8, 16 (“The issue of identifying potential liability arising from the use of an mHealth solution may be complex, because of the numerous actors involved: the manufacturer of the mHealth solution, a healthcare professional, any other care professional involved in the treatment or the electronic communications provider providing the internet. The damage to patient health can come from various sources: a defective device; a wrong diagnosis by the healthcare professional based on inaccurate data; an error by an IT specialist; the patient did not use the device correctly or sent the wrong data to his doctor. This list is not exhaustive and cannot envisage all the possibilities of risks. App developers, mHealth manufacturers and healthcare professionals may request greater legal clarity on the liability risks they may face for having developed or prescribed an app that harmed the user’s health and on the ways to mitigate those risks”).

13 Art 3(f) of the Directive on cross-border healthcare (n 5) defines ‘health professional’ as ‘a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in art 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment’.

transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients'.¹⁴ As such, the concept of telemedicine encompasses both healthcare 'professional-to-patient' relationships (ie, situations where health-related services based on ICTs are provided at distance by healthcare professionals to patients) as well as healthcare 'provider-to-provider' relationships (ie, situations where health-related services based on ICTs are provided at distance by one or more healthcare professionals to one or more healthcare professionals). There are several forms or ways by which telemedicine services may be delivered: telemonitoring,¹⁵ teleintervention,¹⁶ telesurgery,¹⁷ teleconsultation¹⁸ and tele-education.¹⁹ Depending on the relevant medical specialty in which telemedicine services are implemented, telemedicine takes the form of teleradiology, telepsychiatry, teledermatology, telephysiopathology, teleophthalmology, etc.

Thanks to telemedicine it is possible to provide healthcare services beyond traditional physical spaces, including national borders. The independence by physical spaces brings forward a series of advantages: better access to care, especially in case of patients living in remote areas or unable to move (elderly, disabled, inmates), greater timeliness of assistance, greater continuity of assistance for patients with chronic or rare diseases, better management of public health emergencies (such as, for example, the COVID-19 pandemic).²⁰ In other words, healthcare services are provided without the actual movement of the parties (health professionals and/or patients), thanks to communication tools (videoconferencing, email, smartphones or app-enabled technology), and

14 Commission, 'Communication on telemedicine for the benefit of patients, healthcare systems and society' (Communication COM (2008) 689, 3.

15 Telemonitoring is used to enable follow-up or integrated care: health professionals remotely check and monitor the patient's data. These data are collected outside a hospital and may be set either by the patient or by another health professional or automatically by mean of monitoring devices. Telemonitoring can improve the quality of life of chronically ill patients.

16 Teleintervention relates to audiovisual telecommunications between the doctor and the patient.

17 Telesurgery technologies relate to surgical interventions carried out remotely by relying on robotised and computerised machines (such as the da Vinci model). The first long-distance telesurgical operation took place in 2001, when a physician removed the gallbladder of a patient located in France (Strasbourg) from a surgical console located in the United States (New York): on this operation (so-called 'Operation Lindbergh') see Jacques Marescaux and others, 'Transatlantic Robot-Assisted Telesurgery' (2001) 413 *Nature* 379.

18 Teleconsultation is similar to conventional medical consultation with the difference that doctor and patient communicate remotely, through videoconference, phone or chat. Even two or more healthcare professionals can communicate remotely (so-called 'tele-expertise').

19 Tele-education is used to make general and technical information accessible to the general population or other health-care professionals (in this case the so-called 'virtual hospitals' are used).

20 These advantages are accompanied by some critical issues, including the need to reorganise work processes in healthcare institutions and acquire the necessary technological equipment.

store-and-forward or asynchronous technologies that can transmit sensitive clinical data (video or images) collected from patient's wearable devices in order to be clinically evaluated.

By entailing a hyper-personalised and data-driven evaluation of the patient's conditions, telemedicine services raise complex regulatory choices that only partially overlap with those raised by conventional healthcare services. Telemedicine services – that fall, as traditional healthcare services, within the scope of arts 56 and 57 TFEU²¹ – may indeed be characterised simultaneously as 'healthcare' service pursuant to the Directive on cross-border healthcare,²² as well as an 'information society service' (ISS) within the meaning of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter 'eCommerce Directive'²³).²⁴

21 Already at the end of the '90s the ECJ made clear that medical services fall within the concept of 'service' within the meaning of art 57 TFEU, regardless of how the service is delivered; see eg Case C-158/96 *Raymond Kohll v Union des caisses de maladie* [1998] ECR I-01931.

22 Art 3(a) of the Directive on cross-border services (n 5) defines 'healthcare' as 'health services provided by health professionals to patients to assess, maintain or restore their state of health (...)'. Art 1(2) thereof further provides that the Directive applies 'to the provision of *healthcare to patients, regardless of how* it is organised, *delivered* and financed (emphasis added)'. It is to be noted that already in 2003 the Ministers of Health of the Member States of the European Community (EC) and other interested parties invited the European Commission to study how to enhance legal certainty in the area of cross-border healthcare, in accordance with the ECJ's case law. To that effect, healthcare services were originally included in the proposal for the Directive on services in the Internal Market. However, they were ultimately excluded from the scope of the finalized Service Directive (Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [2006] OJ L376/36), as it was deemed preferable to submit a separate proposal to take into account the specificities of the matter; see European Parliament, 'Report on the impact and consequences of the exclusion of health services from the Directive on services in the Internal Market' (Report) 2006/2275(INI).

23 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L 178/1. The application of the eCommerce Directive to telemedicine services is not prejudiced by the Directive on cross-border healthcare (n 5, art 2(e)). The concept of 'information society service' is defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'; *ibid* (eCommerce Directive) art 2(a) and recital n 18; see further art 1(2) of the Directive 98/34/EC of the European Parliament and the Council laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L 204/37 (Regulatory Transparency Directive), repealed by art 1(b) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] OJ L 241.

24 On the characterization of telemedicine as an ISS see Stefaan Callens, 'Telemedicine and the E-Commerce Directive' (2002) 9 *Eur J Health L* 93; Grzegorz Głanowski, 'Legal Status of

In the case of cross-border telemedicine services, ie situations where the health professional and the patient, or more health professionals, are located in different States, several key legal issues arise: licensing/registration of health-care professionals performing telemedicine services;²⁵ conditions for legitimate processing and protection of personal health data;²⁶ respect for the patient's

Telemedicine in the Internal Market' (2016) Eur J Health L 231. As noted by the European Commission, in order to qualify as an ISS, 'the service (...) has to be sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by means of wire, radio, optical means or other electromagnetic means. This means that the following health services are not information society services: services provided in the physical presence of the provider and the recipient, such as medical examinations at a doctor's premises, even if using electronic equipment; services which are not using online telecommunication services, such as a telephone or telefax medical consultation or medical call-centers providing services through traditional voice telephony'; Commission, 'Staff Working Document on the applicability of the existing EU legal framework to telemedicine services' (Staff Working Document) SWD (2012) 414 final, 9. Accordingly, to the extent the telemedicine services qualify as ISS and insofar as they are provided in cross-border context, the regulatory framework of the eCommerce applies to telemedicine services. This legal framework most notably encompasses the 'country of origin' principle (art 3), the principle of responsibility of the Member State where the healthcare provider is established (art 4(1)), the duty of information of ISS providers (art 5), the duty of ISS providers to comply with specific requirements when using commercial communications for the promotion of ISS (arts 6 and 7) and the Member States' obligation to assess whether if healthcare professionals are respecting their professional rules when offering ISS (art 8).

- 25 In this respect, the main problem is whether or not telemedicine service providers have to be licensed/registered in the Member States where the patients are located. Besides the eCommerce Directive and the Directive on cross-border healthcare, the Directive of the European Parliament and the Council 2005/36/EC of 7 September 2005 on the recognition of professional qualifications ([2005] OJ L 255/22) also applies to telemedicine services insofar as health professionals practice a regulated profession under the laws of a Member State.
- 26 See in particular Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector Directive on privacy and electronic communications) [2002] OJ L 201/37 (emended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L 337/11); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1. See also European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (Communication) COM (2022) 197 final.

self-determination;²⁷ reimbursement of the services²⁸. The most problematic

27 Pursuant to art 5 of the 1997 Oviedo Convention on Human Rights and Biomedicine: ‘an intervention in the health field may only be carried out after the person concerned has given free and informed consent to it’. Moreover, the patient ‘shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks [and] (...) may freely withdraw consent at any time.’; Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (opened to signature 4 April 1997, entered into force 1 December 1999), ETS 164 (Oviedo Convention). In telemedicine, patient’s consent is normally given remotely by mean of electronic signature. In some legal orders, the patient has the right to refuse telemedicine services in favor of conventional healthcare services, unless the latter is unavailable due to local conditions and the organization of healthcare services. Worth mentioning is art R6316-2 of the French Public Health Code (*Code de la santé publique*), according to which ‘Les actes de télémedecine sont réalisés avec le consentement libre et éclairé de la personne, en application notamment des dispositions des articles L 1111-2 e L 1111-4. Les professionnels participant à un acte de télémedecine peuvent, sauf opposition de la personne dûment informée, échanger des informations relatives à cette personne, notamment par le biais des technologies de l’information et de la communication.’ In Italy, the 2012 Italian Ministry of Health’s national guidelines on Telemedicine (*Linee di indirizzo nazionali sulla Telemedicina*) read that: ‘It is necessary to clearly bring to the attention of the patient the information necessary to allow a weighted choice. In the particular case of remote services, it is necessary to evaluate the need or not to repeat the consent for each service, and the opportunity to specifically explain the risks that are run (such as, the risks associated with the lack of physical contact and the clinical gaze of the doctor, the impossibility of a complete visit and immediate intervention in an emergency)’. The Italian Ministry of Health’ Decree of 21 September 2022 (*Decreto del Ministero della salute del 21 settembre 2022 Approvazione delle linee guida per i servizi di telemedicina - Requisiti funzionali e livelli di servizio*, 22A06184, GU Serie Generale n 256 del 2 novembre 2022) refers to the ‘informed consent that the patient expresses following appropriate information received which will be prepared by the Ministry of Health in collaboration with the Authority for the protection of personal data and with the regions/PAs, authorizing all the professional figures involved for said treatment’. For an analysis of the issues related to the applicable data protection law see, among others, Jan D Lüttringhaus, ‘Doctors Without Borders? The Law Applicable to Cross-Border eHealth Services and AI-Based Medicine’ in Marcelo Corrales Compagnucci and others (eds), *AI in eHealth: Human Autonomy, Data Governance and Privacy in Healthcare* (CUP 2022) 311, 317.

28 Art 7(7) of the Directive on cross-border healthcare (n 5) provides that: ‘The Member State of affiliation may impose on an insured person seeking reimbursement of the costs of cross-border healthcare, including healthcare received through means of telemedicine, the same conditions, criteria of eligibility and regulatory and administrative formalities, whether set at a local, regional or national level, as it would impose if this healthcare were provided in its territory. This may include an assessment by a health professional or healthcare administrator providing services for the statutory social security system or national health system of the Member State of affiliation, such as the general practitioner or primary care practitioner with whom the patient is registered, if this is necessary for determining the individual patient’s entitlement to healthcare. However, no conditions, criteria of eligibility and regulatory and administrative formalities imposed according to this paragraph may be discriminatory or constitute an obstacle to the free movement of patients, services or goods, unless it is objectively justified by planning requirements relating to the object of ensuring sufficient and permanent access to a balanced range of high-quality treatment in the Member State

profiles, though, are the patients' clinical risk and the liability of healthcare professionals or facilities when patients suffer personal harm in connection with the use of telemedicine services and products. These issues will precisely be the main focus of the following sections.

3. Clinical risk

Clinical risk is the measure of likelihood that patients may incur in adverse events and suffer personal harm in connection with the provided medical treatment. Patients' personal harm may consist *inter alia* in a prolongation of the hospitalisation period, the worsening of health conditions or even death.²⁹ The occurrence of personal harm for patients may be linked to very different kinds of events, actions or omissions. On one hand, personal harm for patients may derive from defects or malfunctioning of the equipment used by professionals to provide medical treatments (eg defects in the manufacturing or a malfunctioning in the use of the relevant equipment, inadequate instructions given by manufacturer, inadequate maintenance through the equipment's lifecycle etc). On the other hand, personal harm for patients may derive either from actions or omissions of healthcare professionals (eg errors in the identification of the relevant patient, delay in diagnosis or medical interventions, operative errors in practicing the relevant treatment, surgical errors etc) or from structural or organizational deficiencies of healthcare facilities (eg shortages of the available medical personnel or medical equipment).³⁰

The occurrence of personal harm for patients may of course trigger civil liability claims. To this effect, civil liability may be divided in 'product' liability and 'professional' liability depending on subject matter of the relevant dispute. Indeed, depending on the factual circumstances of the specific case, the harmed patient could bring civil claim in courts by focusing either on the harm caused by a defective medical equipment or on the harm caused by actions or omissions of healthcare professionals or stemming from healthcare facilities' deficiencies (or a combination thereof).

concerned or to the wish to control costs and avoid, as far as possible, any waste of financial, technical and human resources'.

29 Linda T Kohn, Janet M Corrigan and Molla S Donaldson (eds), *To err is human: building a safer health system* (National Academy Press Washington 1999) X.

30 *ibid*: '(...) errors are responsible for an immense burden of patient injury, suffering and death. Second, errors in the provision of health services, whether they result in injury or expose the patient to the risk of injury, are events that everyone agrees just shouldn't happen. Third, errors are readily understandable to the American public. Fourth, there is a sizable body of knowledge and very successful experiences in other industries to draw upon in tackling the safety problems of the health care industry. Fifth, the health care delivery system is rapidly evolving and undergoing substantial redesign, which may introduce improvements, but also new hazards'.

Both types of civil liability claims may in turn involve several national legal systems. Consider for instance the case in which a professional located in State A performs robotic surgery on a patient citizen of State B (domiciled and resident in State C) using equipment designed in State D and manufactured in State E. If personal harm occurs, the patient's claim potentially involves both types of liability and five legal systems.³¹ To the extent that a dispute concerning product liability and/or health professionals' liability in the context of telemedicine and eHealth touches upon different legal orders, private international law issues come into play. Based on the distinction between product liability and health professionals' liability, the following sections (4.–5.) assess the extent of substantive harmonisation achieved at EU-wide level and the role played by the general instruments of EU private international law to address potential conflicts of jurisdiction and of laws. The paper ends with some concluding remarks (6.).

4. Product liability

4.1. Harmonised substantive rules

As far as liability for defective products is concerned, ever since the '80s the European Community (EC) has established harmonised rules through the Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products³² (hereinafter the 'Product Liability Directive'). This Directive has established the principle of objective liability – strict or faultless liability – of the producer/importer as well as of the supplier insofar as the producer/importer cannot be identified. The EU legislator considers the imposition of a strict liability regime upon producers to be 'the sole means of adequately solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production'.³³ When more than one person is liable for the same damage, joint and several liability applies and the injured person (usually the patient) is entitled to claim full compensation for the damage suffered by any one of the liable persons (art 5). To establish liability for defective products, the injured person has to prove the damage, the defect and the causal relationship between defect and damage (art 4), without being required to further demonstrate the existence

31 See Bernard M Dickens and Rebecca J Cook, 'Legal and ethical issues in telemedicine and robotics' (2006) 94 *Intl J Gynecology and Obstetrics* 73.

32 [1985] OJ L 210/29, subsequently amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 [1999] OJ L 141/20.

33 *ibid*, recital n 2.

of fault or negligence on behalf of the liable person. Producer's liability may only be excluded or reduced under rather strict circumstances (arts 7 and 8). Member States shall provide in their legislation that a limitation period of three years applies to proceedings for the recovery of damages (the limitation period shall begin to run from the day on which the plaintiff became aware, or should reasonably have become aware, of the damage, the defect and the identity of the producer) as well as that the rights conferred upon the injured person shall be extinguished upon the expiry of a period of ten years from the date on which the producer put into circulation the actual product which caused the damage (arts 10 and 11). Moreover, the strict liability regime established under the Directive does not affect the rights granted to the injured person under the Member States' rules of the law of contractual or non-contractual liability (art 13).

The Product Liability Directive only applies to tangible products (art 2). By contrast, it does not cover software and other intangible digital assets, which – as already mentioned – are of fundamental importance for the provision of telemedicine and eHealth services.

Precisely to fill the regulatory gap concerning the liability for emerging digital technologies and AI-based systems, in 2018 the European Commission delivered an interesting Working Document³⁴ which was subsequently followed by the presentation in 2022 of a package of proposals for directives aiming to adapt the liability rules to the digital age. To that effect, the European Commission proposed the adoption of two distinct yet complementary acts, one dealing with liability for defective products³⁵ and the other one with the liability for damages caused by AI systems. Both the instruments should have had the effect of integrating the EU legislation on the safety and performance of medical

34 Commission, 'Liability for emerging digital technologies' (Staff Working Document) SWD (2018) 137 final.

35 European Commission, 'Proposal for a Directive on liability for defective products' (Communication) COM (2022) 495 final. The Explanatory Memorandum attached to the proposal addresses *inter alia* the relationship between the proposal itself, the Product Liability Directive (PLD) and national liability regimes. In this regard, it emphasizes that: 'national liability regimes exist in each Member State that allow compensation claims in more situations than under the PLD: claims can be made against a broader range of liable persons for a broader range of damages. These claims cover services as well as products, and often allow more time to make a claim. However, injured persons have to prove the wrongdoer's fault, which is not required under the PLD. The PLD, as a no-fault (strict) liability regime, does not affect these rights, so the PLD is consistent with the broader national regimes...The draft Directive on adapting non-contractual fault-based civil liability rules to artificial intelligence, adopted as a package with this proposal, seeks to facilitate access to information and alleviate the burden of proof in compensation claims pursued under national fault-based liability regimes in cases where certain AI systems are involved in causing damage. There is no overlap with claims brought under the PLD'.

devices (including AI-based medical devices) envisaged by the Regulation (EU) 2017/745 of 5 April 2017 on medical devices.³⁶

In 2024 the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, hereinafter the ‘AI Act’) and the Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products were actually adopted.

As for this Directive³⁷, the most relevant novelty for the purpose of the liability of providers of telemedicine services lies in the expansion of the concept of ‘product’. This notion is no longer limited to tangible products and is extended as to encompass ‘digital manufacturing files ... and software’.³⁸ The

36 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1.

For an analysis see Sofia Palmieri, Paulien Walraet and Tom Goffin, ‘Inevitable Influences: AI-Based Medical Devices at the Intersection of Medical Devices Regulation and the Proposal for AI Regulation’ (2021) 28 Eur J Health L 341. The Medical Devices Regulation makes clear that softwares are included among the medical devices covered by the Regulation’s scope of application when the software manifests itself as a stand-alone medical device or when is integrated in a medical device based on AI systems. Under Directive 93/42/EEC (now repealed by the Medical Devices Regulation), the ECJ clarified that ‘software, of which at least one of the functions makes it possible to use patient-specific data for the purposes, inter alia, of detecting contraindications, drug interactions and excessive doses, is, in respect of that function, a medical device (...) even if that software does not act directly in or on the human body’; Case C–329/16 *Syndicat national de l’industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé* [2017] ECLI:EU:C:2017:947. The preamble of the Medical Devices Regulation makes clear that: ‘where, in the course of a clinical investigation, harm caused to a subject leads to the civil or criminal liability of the investigator or the sponsor being invoked, the conditions for liability in such cases, including issues of causality and the level of damages and sanctions, should remain governed by national law’ (recital n 66). Art 69 provides that: ‘Member States shall ensure that systems for compensation for any damage suffered by a subject resulting from participation in a clinical investigation conducted on their territory are in place in the form of insurance, a guarantee, or a similar arrangement that is equivalent as regards its purpose and which is appropriate to the nature and the extent of the risk’.

37 [2024] OJ L 2853/1.

38 *ibid* art 4(1). Recital 13 reads that: ‘Products in the digital age can be tangible or intangible. Software, such as operating systems, firmware, computer programs, applications or AI systems, is increasingly common on the market and plays an increasingly important role for product safety. Software is capable of being placed on the market as a standalone product or can subsequently be integrated into other products as a component, and it is capable of causing damage through its execution. In the interest of legal certainty, it should be clarified in this Directive that software is a product for the purposes of applying no-fault liability, irrespective of the mode of its supply or usage, and therefore irrespective of whether the software is stored on a device, accessed through a communication network or cloud technologies, or supplied through a software-as-a-service model. Information is not, however, to be considered a product, and product liability rules should therefore not apply to the content of

overarching aim of the Directive is to establish EU-wide uniform rules enabling persons who suffered personal or financial injury as a result of defective AI systems to more easily claim compensation from the supplier of the AI system or from the manufacturer who integrated an AI system into another product. To that effect, art 10 sets out particularly relevant provisions on the burden of proof. On one hand, it lays down the conditions under which the defectiveness of the product shall be presumed (art 10(2)) and, on the other hand, it establishes the presumption about the existence of the causal link between the defectiveness of the product and the damage ‘where it has been established that the product is defective and the damage caused is of a kind typically consistent with the defect in question’ (art 10(3)).

The AI Act³⁹ involves a very complex and technical discipline. As far as we are concerned, it is enough to remember here that it categorizes AI systems according to the level of risk associated with them (by “risk” is meant “the combination of the probability of an occurrence of harm and the severity of that harm”) and pays particular attention to prohibited AI practices (art 5) and high-risk AI systems (art 6)⁴⁰ including those used in healthcare services

digital files, such as media files or e-books or the mere source code of software. A developer or producer of software, including AI system providers within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council, should be treated as a manufacturer’.

39 [2024] OJ L 1689/1.

40 “High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. On the basis of the New Legislative Framework, as clarified in the Commission notice “The “Blue Guide” on the implementation of EU product rules 2022”, the general rule is that more than one legal act of Union harmonisation legislation, such as Regulations (EU) 2017/745 (on medical devices) and (EU) 2017/746 (on *in vitro* diagnostic medical devices) ... may be applicable to one product, since the making available or putting into service can take place only when the product complies with all applicable Union harmonisation legislation. To ensure consistency and avoid unnecessary administrative burdens or costs, providers of a product that contains one or more high-risk AI systems, to which the requirements of this Regulation and of the Union harmonisation legislation listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all applicable requirements of the Union harmonisation legislation in an optimal manner. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation should minimise any potential restriction to international trade” (recital 46). “AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its

(Annex III, point 5 (a) and (d)). The inclusion of AI systems for use in the medical field among those classified as high risk is not without significant implications for operators in the sector, ie for manufacturers, distributors, retailers and deployers⁴¹.

4.2. Conflicts of jurisdiction

In the absence of more specific EU legislation, the allocation of adjudicative jurisdiction between Member States' courts over civil claims arising out of the alleged infringement of product liability rules in the context of telemedicine or eHealth products and devices is governed by the Council Regulation (EU) 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) (hereinafter 'Brussels I-bis Regulation').⁴²

As far as product liability disputes arising out of telemedicine products are concerned, the Brussels I-bis Regulation is likely to simultaneously attribute jurisdiction to the courts of different Member States. Although the rules on exclusive jurisdiction lay down in art 24 thereof may hardly be of any relevance in this context, exclusive jurisdiction could in principle derive from a choice-of-court agreement eventually concluded between the parties (art 25). If the relevant choice-of-court agreement does not confer exclusive jurisdiction or such an agreement had not been concluded at all, jurisdiction of the court seized could also be based on the defendant's appearance in the forum (art 26) or on the application of the special rules aimed at protecting the claimant as a weaker party in his relationship with the defendant, most notably those applicable to consumer contracts (arts 17–19). More realistically, the injured party will have to resort, at his or her choice, either to the general forum of the defendant's domicile (art 4) or, since product liability disputes very often arise in the absence of a contract linking the interested parties, to the special *forum delicti* (art 7(2)). Art 7(2) applies to claims generally relating to 'tort, delict or quasi-delict' and vests jurisdiction upon the courts of the place where the 'harmful event' occurred or may occur, a notion that for distance torts encompasses both the place where

digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate" (recital 47).

41 Regarding aspects relating to civil liability see Søren Holm, Catherine Stanton and Benjamin Bartlett, 'A New Argument for No-Fault Compensation in Health Care: The Introduction of Artificial Intelligence Systems' (2021) 29 Health Care Analysis 171; and, more generally, Benedetta Cappiello, *AI-systems and non-contractual liability. A European private international law analysis* (Giappichelli 2022).

42 [2012] OJ L 351/1.

the event giving rise to the damage (*forum actus*) and the place of the damage (*forum damni*) occurred or may occur.⁴³ As regard product liability torts claims, the ECJ case law has localized the *forum actus* at the place where the relevant product had been manufactured.⁴⁴ Admittedly, the *forum actus* very often does not offer any meaningful alternative for prospective plaintiffs to the general forum of the defendant's domicile. By contrast, the *forum damni* may offer interesting alternatives for prospective plaintiffs, by often enabling them to bring proceedings in their own 'home' forum and in other additional fora.⁴⁵ For product liability torts, the ECJ case law seems to localize the *forum damni* in the place where the initial damage occurred as a result of the normal use of the product, provided that the relevant product was purposefully marketed in that place.⁴⁶

A product liability claim could eventually be assigned by the injured individual to another person acting as a claimant or could be brought by a representative entity on the individual's behalf (eg non-profit organizations, associations, bodies etc): this is the so-called 'collective redress'⁴⁷. To this effect, the EU legislator has adopted the Directive (EU) 2020/1828 of 25 November 2020 on representative actions for the protection of the collective interests of consumers (repealing Directive 2009/22/EC).⁴⁸ The directive lays down some minimum harmonisation rules by obliging the Member States to provide at least one procedural mechanism enabling representative entities that fulfill certain qualifying requirements to bring claims for injunction and compensation on behalf of individual consumers.⁴⁹ This procedural mechanism must be available for claims arising out of alleged infringements of a long list of EU law instruments insofar as the infringement affects or may affect consumers' general interests.⁵⁰ Such a list includes *inter alia* the Medical Device Regulation.⁵¹ Since the Directive

43 Ever since Case 21/76 *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA* [1976] ECR 1735, paras 12–25.

44 Case C–45/13 *Andreas Kainz v Pantherwerke AG* [2014] ECLI:EU:C:2014:7, paras 26–29 and 33.

45 eg Jan von Hein, 'Protecting Victims of Cross-Border Torts under Article 7 No. 2 Brussels Ibis: Towards a more Differentiated and Balanced Approach' (2015) XVI Yearb priv int law 241; Etienne Farnoux, 'Delendum est Forum Delicti? Towards the Jurisdictional Protection of the Alleged Victim in Cross-Border Torts' in Burkhard Hess and Koen Lenaerts (eds), *The 50th Anniversary of the European Law of Civil Procedure* (Nomos 2020) 259.

46 Case C–189/08 *Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA* [2009] ECR 2009 I-06917, paras 25–32; Case C–343/19 *Verein für Konsumenteninformation v Volkswagen AG* [2020] ECLI:EU:C:2020:534, paras 32–40.

47 See generally Alexia Pato, *Jurisdiction and Cross-Border Collective Redress: A European Private International Law Perspective* (Hart Publishing 2019).

48 [2020] OJ L 409/1.

49 *ibid* arts 1–2, 4, 7–9. See further recitals n 7, 10–12, 24–31, 40–51.

50 *ibid* art 2(1) and Annex I.

51 Medical Devices Regulation (n 36), *ibid* (Annex I) point 57.

applies in principle to both domestic and transnational representative actions,⁵² it may to some extent facilitate the conditions under which injured persons may bring cross-border collective proceedings against e-Health services providers for alleged infringements of provisions of EU law on medical devices. Yet, the Directive neither affects the existing private international law rules on jurisdiction, choice of law and recognition/enforcement of judgments nor establishes such rules.⁵³ As such, the Brussels I-bis Regulation remains fully applicable with respect to collective product liability claims in the context of eHealth products and devices. Unfortunately, the Brussels I-bis Regulation has long been acknowledged in literature as being built upon a traditional conception of two-party proceedings, a tenet that the ECJ case law has carefully and constantly safeguarded.⁵⁴ For the time being, the only rule on jurisdiction enshrined in the Brussels I-bis Regulation that may constitute a solid ground of jurisdiction for collective redress proceedings is general forum of the defendant's domicile (art 4).⁵⁵ Although the *forum damni* under art 7(2) as an alternative to the general rule based on art 4 remains in principle available,⁵⁶ its application to collective redress proceedings suffer significant drawbacks primarily because of the consolidated principle in the ECJ case law that special jurisdiction needs to be determined independently and separately for each claimant and each claim.⁵⁷

52 *ibid* arts 2(1), 3(6)–(7) and 4(1)–(2).

53 *ibid* art 2(3), recital n 21.

54 *eg* Arnaud Nuyts, 'The Consolidation of Collective Claims Under Brussels I' in Arnaud Nuyts and Nikitas E Hatzimihail (eds), *Cross-Border Class Actions: The European Way* (Sellier European Law Publishers 2013) 69; Burkhard Hess, 'Collective Redress and the Jurisdictional Model of the Brussels I Regulation' in Arnaud Nuyts and Nikitas E Hatzimihail (eds), *Cross-Border Class Actions: The European Way* (Sellier European Law Publishers 2013) 59; T M C Arons, 'Cross-border dimension of collective proceedings in the Brussels Ibis regime: jurisdiction, *lis pendens* and related actions' in Peter Mankowski (ed), *Research Handbook on the Brussels Ibis Regulation* (Edward Elgar Publishing 2020) 1; Frederick Rielaender, 'Aligning the Brussels Regime with the Representative Actions Directive' (2022) 71 ICLQ 107.

55 *ibid*.

56 *eg* Case C–167/00 *Verein für Konsumenteninformation v Karl Heinz Henkel* [2000] ECLI:EU:C:2002:555; Case C–191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] ECLI:EU:C:2016:612; Case C–343/19 *Verein für Konsumenteninformation v Volkswagen AG* [2020] ECLI:EU:C:2020:534.

57 Case C–147/12 *ÖFAB, Östergötlands Fastigheter AB v Frank Koot and Evergreen Investments BV* [2013] ECLI:EU:C:2013:490, para 58; C–352/13 *Cartel Damage Claims (CDC) Hydrogen Peroxide SA v Evonik Degussa GmbH and Others* [2015] ECLI: EU:C:2015:335, paras 35–36; Case C–498/16 *Maximilian Schrems v Facebook Ireland Limited* [2018] ECLI:EU:C:2018:37, para 48. Several scholars consider the topic of jurisdiction over collective redress proceedings as one of the key aspects in respect of which the Commission should propose amendments to the Brussels I-bis Regulation; *eg* Burkhard Hess and others, 'The Reform of the Brussels Ibis Regulation' (2022) 6 MPILux Research Paper Series 1; Rielaender (n 54) 110.

4.3. Conflict of laws

The aforementioned instruments of EU law only address limited aspects of the several substantive legal issues relating to product liability in the context of eHealth products and devices. To the extent that uniform substantive rules had not been established at EU and international level, national courts of the EU Member States will have to solve conflicts between national product liability regimes primarily by reference to the general instruments of EU private international law, and most notably by reference to the Council Regulation (CE) 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II Regulation)⁵⁸. Unlike the Brussels I-bis, the Rome II Regulation includes some provisions specifically applicable to matters of product liability (art 5). Based on the *lex specialis* principle, the specific conflict-of-law rules enshrined in art 5 supplants the Rome II Regulation's general conflict-of-law rule according to which the law applicable to non-contractual obligations is the law of the place where the damage occurs (art 4(1)). The conflict-of-law rules enshrined in art 5 are underlined by the 'objectives of fairly spreading the risks inherent in a modern high-technology society, protecting consumers' health, stimulating innovation, securing undistorted competition and facilitating trade.'⁵⁹ To strike a fair balance between these objectives, art 5(1) provides for a 'cascade systems connecting factors, together with a foreseeability clause.'⁶⁰ The conflict-of-law rules enshrined in art 5(1) only applies if the parties to the dispute have their habitual residence in different countries.⁶¹ The *lex causae* identified by reference to the connecting factors under art 5(1) may exceptionally be displaced by the law of another country with which the relevant tort is manifestly more closely connected in the light of all the circumstances of the specific case (art 5(3)). The cascade of connecting factors identified in art 5(1) is largely built upon the criterion of the 'marketing' of the product.⁶² First of all, the law of the allegedly injured person's habitual residence applies if the product was marketed in that country. If the injured person does not have his or her habitual residence

58 [2007] OJ L 199/40. See Paola Ivaldi, 'Civil Liability for Health Damages and Uniform Rules of Private International Law' (2017) 53 *Rivista di diritto internazionale privato e processuale* 857. Some EU Member States (France, Spain, Croatia, Slovenia, Finland, the Netherlands and Luxembourg) have ratified the Convention of 2 October 1973 on the Law Applicable to Products Liability of 2 October 1973 (entered into force 1 October 1977) (Hague Products Liability Convention). Under art 28(1) Rome II, this Convention takes precedence over the Rome II Regulation; Piotr Machnikowski 'Art 5 - Chapter II: Torts/Delicts' in Ulrich Magnus and Peter Mankowsky (eds), *Volume 3 Rome II Regulation – Commentary* (Verlag Dr. Otto Schmidt 2019) 212.

59 *ibid* recital n 20, first sentence.

60 If the parties habitually reside in the same country, the law of the parties' common habitual residence applies (art 4(2)).

61 Art 5 Rome II Regulation applies 'without prejudice to Article 4(2)' thereof; *ibid* art 5(1).

62 Piotr Machnikowski (n 58) 218.

within the country where the product was marketed, the law of the country of ‘marketing’ applies when the product was acquired in that country (art 5(1)(b)), or failing that, the damage occurred in that country (art 5(1)(c)). In any event, the law applicable on the basis of art 5(1)(a)–(c) is displaced by the law of the country where the alleged tortfeasor habitually resides if he or she could not reasonably foresee the circulation of the product in either of the countries mentioned under letters (a)–(c) (art 5(1)2). The applicable law will determine the basis and the extent of liability, the level of compensation and the nature and the assessment of the damage.

5. Health professional’s liability

5.1. Harmonised substantive rules

As already anticipated, the harm suffered by patients could derive from a misconduct of health professionals or from more structural and organizational deficiencies in healthcare facilities. Accordingly, for the purpose of the present paper, the very concept ‘health professional’s liability’ should be understood widely as to encompass the liability arising from ‘medical treatment’, that in turn encompasses all health measures aimed at improving the patient’s health conditions. As such, health professional’s liability encompasses the liability arising from both health professionals’ misconducts (eg wrongful diagnosis and/or operative errors in practicing the relevant treatment) and from more structural and organizational deficiencies of the healthcare facilities (eg shortages of medical staff and/or inadequate organizational choices).

The health professional’s civil liability arising from health treatments provided through telemedicine and eHealth devices raises delicate and complex substantive legal issues in a cross-border context. Typical substantive legal issues which could arise include issues about apportionment of liability between the health professionals and the producers of telematic devices/services (eg failure of the health treatment because of the device’ loss of connectivity), the extent of health professionals’ discretion in choosing between a conventional treatment or a treatment based on ICTs devices (eg health professional’s choice of resorting to telemedicine in a situation where it would have been more appropriate to resort to conventional medicine or vice versa), issues about the type and the extent of fault required for establishing the health professional’s liability and whether or not reliance on telemedicine should require different insurance regimes than those applicable to conventional medicine.

The Directive on cross-border healthcare contains some helpful provisions, albeit clearly not solving all substantive legal issues that could arise in connection with the cross-border provision of telemedicine services. The Directive

lays down certain obligations for the Member State where the health treatment is provided (the ‘Member State of treatment’). As far as conventional medicine is concerned, the ‘Member State of treatment’ is the Member State on whose territory healthcare is provided to the patient (art 3(1)(d), first sentence). As regard telemedicine, the Directive provides that ‘healthcare is considered to be provided in the Member State where the healthcare provider is established’ (art 3(1)(d), second sentence). As such, with respect to telemedicine services the Directive seems to establish a legal fiction according to which the patient should be treated as if he or she has moved from the territory of the Member State where the treatment was actually provided to the Member State of establishment of the healthcare’s provider. The Directive provides that, ‘taking into account the principles of universality, access to good quality care, equity and solidarity, cross-border healthcare shall be provided in accordance with: (a) the legislation of the Member State of treatment; (b) standards and guidelines on quality and safety laid down by the Member State of treatment; and (c) Union legislation on safety standards’ (art 4(1)).⁶³ The Directive then specifies that the Member State of treatment shall ensure that ‘healthcare providers provide relevant information to help individual patients to make an informed choice, including on treatment options, on the availability, quality and safety of the healthcare they provide in the Member State of treatment and that they also provide clear invoices and clear information (...) on their insurance cover or other means of personal or collective protection with regard to professional liability’; that ‘there are transparent complaints procedures and mechanisms in place for patients, in order for them to seek remedies in accordance with the legislation of the Member State of treatment if they suffer harm arising from the healthcare they receive’ and that ‘systems of professional liability insurance, or a guarantee or similar arrangement that is equivalent or essentially comparable as regards its purpose and which is appropriate to the nature and the extent of the risk, are in place for treatment provided on its territory’ (art 4(2) (b)–(d)). Patients should receive from the national contact point of the Member

63 Recital n 49 further reads that: ‘when a patient receives cross-border healthcare, it is essential for the patient to know in advance which rules will be applicable. The rules applicable to cross-border healthcare should be those set out in the legislation of the Member State of treatment, given that, in accordance with art 168(7) TFEU, the organisation and delivery of health services and medical care is the responsibility of the Member States. This should help the patient in making an informed choice, and should avoid misapprehension and misunderstanding. It should also establish a high level of trust between the patient and the healthcare provider.’ It should be pointed out, though, that the rules on the free provision of services contained in Directive 2005/36/EC of 7 September 2005 on the recognition of professional qualifications do not apply if the patient does not move to another Member State than that of his or her habitual residence to receive the healthcare service. As made clear by art 5(2), in fact, the Directive on the recognition of professional qualifications ‘shall only apply where the service provider moves to the territory of the host Member State to pursue, on a temporary and occasional basis, the profession’.

State of treatment, upon request, a) relevant information on the standards and guidelines on quality and safety laid down by the Member State of treatment, 'including provisions on supervision and assessment of healthcare providers, information on which healthcare providers are subject to these standards'; b) 'relevant information to help individual patients to make an informed choice, including on treatment options, on the availability, quality and safety of the healthcare they provide in the Member State of treatment and ... clear information on prices, ... insurance ... or other means of personal or collective protection with regard to professional liability' (art 4(2)(a)–(b)). Failure to provide such information could also have a role in establishing the liability of actors involved in the provision of cross-border healthcare services.⁶⁴

Intermediary healthcare service providers are subject to the provisions of the eCommerce Directive establishing a gradual liability scheme for intermediaries of information society services (arts 12–15). Patients may indeed have an interest in suing intermediary healthcare service providers, rather than persons or entities directly responsible for making available certain contents or information on a given Internet-based device (eg producers or designers). Thus, for instance, when the harm suffered by the patient is due to the loss of online connectivity of the relevant telemedicine device, liability for such harm could also lie upon the competent Internet service provider and not only upon the relevant producer or designer of the relevant Internet-based telemedicine devices.

Nevertheless, the protective provisions set forth in the Directive on Consumer Rights 2011/83/EC⁶⁵ are not applicable to patients of healthcare services. Indeed, the Directive explicitly excludes contracts for the provision of healthcare services from its scope of application (art 3(3)(b))⁶⁶ on the ground that 'healthcare requires special regulations because of its technical complexity, its importance as a service of general interest as well as its extensive public funding' (recital 30).

5.2. Conflicts of jurisdiction

Matters of international jurisdiction are not specifically dealt with by both the Directive on cross-border healthcare and the eCommerce Directive. On one hand, the Directive on cross-border healthcare applies 'without prejudice to (...) Union rules on private international law, in particular rules related to court jurisdiction' (art 2(q)). On the other hand, in the same vein, the eCommerce

64 Commission (n 24), 20–21.

65 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L 304/64.

66 A similar exclusion, though, cannot be found in the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.

Directive ‘does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts’ (art 1(4) and recital 23). Accordingly, international jurisdiction over civil claims arising out of health professionals’ liability in the context of telemedicine should, once again, be determined by reference to the Brussels I-bis Regulation.

With the view of providing guidance on how the Brussels I-bis Regulation should apply to those claims, the European Commission draws a distinction between three different scenarios involving the cross-border provision of telemedicine services.⁶⁷ In all three scenarios claimants may generally avail themselves of jurisdiction at the general forum of defendant’s domicile (art 4 Brussels I-bis) as well as of the jurisdiction of courts identified through a choice-of-court agreements eventually concluded with the other party (art 25). Besides these fora, the applicable grounds of jurisdiction under the Brussels I-bis Regulation will depend on the nature of the legal relationship existing between the relevant parties to the dispute. The first scenario identified by the Commission relates to situations where cross-border telemedicine involves health professionals/physicians and other eHealth providers only (ie professional-to-professional relationships). In this scenario, the claimant may avail himself or herself of the *forum contractus* (art 7(1)(b)), so that he or she will be able to bring proceedings before the court of the place where, under the contract, the services were provided or should have been provided.⁶⁸ The second scenario relates to legal relationships between healthcare professionals and patients (professional-to-patient relationships). According to the Commission, the patient, to the extent the professional’s activity is directed to the Member State of the patient’s domicile, may avail himself or herself of jurisdiction of the courts of the Member State of his or her domicile pursuant to protective rules on jurisdiction applicable to consumer contracts (art 18(1)).⁶⁹ If the professional does not ‘direct’ its activities to the patient’s domicile pursuant to the ECJ case law,⁷⁰ the patient may avail himself or herself of the jurisdiction of

67 Commission (n 24), 24ff.

68 *ibid* 25.

69 *ibid*.

70 *ibid*, the European Commission (*ibid*) makes reference to the ‘targeting’ test relied upon by the ECJ in *Pammer and Alpenhof* for establishing whether the trader has ‘directed’ its activity to the consumer’s domicile pursuant to art 17(1)(c) Brussels I-bis, as a precondition for triggering the application of the rules on jurisdiction for the protection of consumers under art 18–19 Brussels I-bis; Joined Cases C–585/08 and C–144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECR 2010 I-12527, paras 80–94. According to the ECJ, attention should be given to a non-exhaustive list of factors, such as ‘the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure

the competent court pursuant to the *forum contractus* (art 7(1)(b)).⁷¹ The third and last scenario considered by the Commission is the legal relationship between a patient and a specialist consulted by the reference professional (who, for example, for a more accurate interpretation, sends him the images on the basis of a teleradiology services contractual relationship between the hospitals to which they belong). In this situation the patient may avail himself or herself of the *forum delicti* (art 7(2)). According to the Commission, the place where the event giving rise to the damage occurred (*forum actus*) should be localized in the Member State where the professional is located when delivering the service, whereas the place where the damage occurred (*forum damni*) shall be located in the Member State where the patient was located when he received the medical advice or treatment.⁷²

In some parts the reconstruction made by the Commission might not be entirely convincing and its solidity could be questioned. First of all, such a reconstruction is based on the undemonstrated assumption that the relationship between the patient and the healthcare professional is to be generally characterized as ‘contractual’ in nature. Yet, comparative legal analysis would not so decisively point towards a ‘contractual’ characterization of such a relationship. For instance, the German legal system, whose main focus had traditionally been centered over the patient’s absolute right to physical integrity and life, tends

on an internet referencing service in order to facilitate access to the trader’s site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States’. On the other, the ECJ stressed that the ‘mere accessibility of the trader’s or the intermediary’s website in the Member State in which the consumer is domiciled is insufficient.’ In literature, ‘targeting’ tests, such as the one established by the ECJ in *Pammer*, are very often regarded as rather viable solutions for geographically localizing (ubiquitous and borderless) digital and Internet-based activities; eg Tobias Lutz, *Private International Law Online. Internet Regulation and Civil Liability in the EU* (OUP 2020) 145–147. For the time being, the ECJ has limited the scope of such a ‘targeting’ test only to the Brussels I-bis’ jurisdictional provisions for consumers’ protection and has largely refused to rely on it under other grounds of jurisdiction that often comes into play in respect to Internet-based activities, most notably the *forum delicti* under art 7(2); eg Case C–170/12 *Peter Pinckney v KDG Mediatech AG* [2013] ECLI:EU:C:2013:635, para 42; Case C–251/20 *Giffix Tv v DR* [2021] ECLI:EU:C:2021:1036, paras 41–42. The ECJ justifies the rejection of ‘targeting’ under art 7(2) on the basis of the textual argument that this latter provision, differently than art 17(1)(c), does not require the defendant’s activity to be ‘directed’ towards the competent forum. However, the reason of such a rejection is probably to be found in the difficult conciliation between the flexibility characterizing ‘targeting’ tests and the consolidated principle in the ECJ case law that the grounds of jurisdiction under the Brussels I regime should be highly predictable for the parties to the dispute and promptly applicable by Member States’ courts; Edina Márton, *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law* (Nomos 2016) 251; cf Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017) 81–82.

71 Commission (n 24), 25.

72 *ibid.*

to position professional-to-patient relationships within the boundaries of the *Deliktmaterie*. In any event, it should also be emphasized that professional-to-patient relationships are increasingly mediated by healthcare institutions and infrastructures (either public or private), so that a contractual relationship could eventually be deemed to exist, if at all, between the patient and the healthcare institution, rather than between patient and professional practicing within such an institution. Similarly to the German legal system, also the Italian legal system, albeit slightly less markedly, points in the direction of characterizing professional-to-patient relationships as ‘non-contractual’ in nature. In more recent times, that system has to some extent moved towards a ‘contractualization’ of medical liability. This is especially the case for relationships involving patients and self-employed physicians, on one hand, and relationships involving patients and healthcare institutions acting as employers of the relevant physicians, on the other hand. Yet, also under the Italian legal system, the ‘non-contractual’ characterization of medical liability persists as regard relationships between patients and physicians acting as employees of healthcare institutions. Regardless of the foregoing, admittedly, it seems hardly feasible to identify a common ground among different EU Member States about the contours of medical liability and its characterization as ‘contractual’ or ‘non-contractual’. For drawing the line between ‘contractual’ and ‘non-contractual’ matters within the general instruments of EU private international law, the ECJ qualifies as ‘contractual’ any ‘legal obligation freely consented to by one person towards another’ and defines ‘non-contractual’ matters negatively and residually as encompassing ‘all actions which seek to establish the liability of a defendant and are not related to a contract’.⁷³ On this basis, the ECJ case law generally suggests a preference for the ‘contractual’ characterization.⁷⁴ However, the ECJ has not yet been specifically faced with issues relating to the characterization of medical liability, nor any clear guidance on this issue may be inferred from its general case law. Even if it is to be assumed that medical liability should be characterized as ‘contractual’ in nature from the perspective of EU private international law - a solution

73 Under the Brussels I regime see, seminally, Case C-26/91 *Jakob Handte & Co. GmbH v Traitements Mécano-chimiques des Surfaces SA* [1992] ECR 1992 I-3967, para 15; Case C-189/87 *Athanasios Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co. and others* [1988] ECR 1988 05565, para 18. Under the Rome I and II regulations see, eg Joined Cases C-359/14 and C-475/14 *‘ERGO Insurance’ SE v ‘If P&C Insurance’ AS and ‘Gjensidige Baltic’ AS v ‘ZU Lietuva’ UAB DK* [2016] ECLI:EU:C:2016:40, paras 42–46. In literature: Alfonso-Luis Calvo Caracava and Javier Carrascosa González, ‘Art 1 - Chapter I: Scope’ in Ulrich Magnus and Peter Mankowsky (eds), *Volume 2 Rome I Regulation – Commentary* (Verlag Dr. Otto Schmidt 2016) 62–72; Peter Mankowsky, ‘Art 1 - Chapter I: Scope’ in Ulrich Magnus and Peter Mankowsky (eds), *Volume 3 Rome II Regulation – Commentary* (Verlag Dr. Otto Schmidt 2019) 69–90; Marta Requejo Isidro, Edith Wagner and Matteo Gargantini, ‘Art 7’ in Marta Requejo Isidro (ed), *Brussels I Bis: A Commentary on Regulation (EU) No 1215/2012* (Edward Elgar Publishing 2022) 94–103 and 112–115.

74 *ibid*, see also Burkhard Hess, *Europäisches Zivilprozessrecht* (De Gruyter 2021) 6.55.

that may be questioned from a comparative assessment of the EU Member States' legal systems - further doubts may arise as regard to the characterization of the contract for the provision of healthcare services as a 'consumer' contract. The outright solution of characterizing patients as a 'consumers' pursuant to Brussels I-bis Regulation, as pointed out to by the Commission, might be deemed hardly reconcilable with the contextual approach followed by the ECJ in this respect⁷⁵. Moreover, the solution of characterizing contracts for the provision of healthcare services as 'consumer' contracts could also be questioned in the light of the EU's legislator choice under Directive on Consumer Rights 2011/83/EC to exclude contracts for the provision of healthcare services from its scope of application because of the specificities of the healthcare sector.

As for the figure of the doctor consulted, it is not excluded that it could be equated to the auxiliary, so that the structure/consultant doctor would be liable for any damage. Finally, we cannot ignore the need – felt in many States – to curb the excess of responsibility to which the medical profession is exposed, while at the same time contrasting the excess of defensive medicine practices.⁷⁶ In fact, an increasing number of systems (including France⁷⁷ and Belgium⁷⁸) envisage alternative social security systems which – as already the defective products Directive – disregard the ascertainment of non-fulfillment or fault (so-called no-fault systems), favor the compensatory function of the damage (to the detriment of the deterrent one) and are characterised by quantitatively lower refreshments.

5.3. Conflict of laws

In the absence of a uniform substantive regulation of health professionals' liability at EU and international level, conflict of laws matters will to a large extent have to be solved again by reference to the general instruments of EU private international law. On one hand, the Directive on cross-border healthcare applies 'without prejudice to (...) Union rules on private international law (...)' (art 2(q)). On the other, the eCommerce Directive does not establish additional private international law rules but simply requires the Member States to ensure that, within eCommerce Directive's 'coordinated field', providers of

75 eg Stephanie Law, 'Art 17' in Marta Requejo Isidro (ed), *Brussels I Bis: A Commentary on Regulation (EU) No 1215/2012* (Edward Elgar Publishing 2022) 253–267.

76 The concept of defensive medicine refers to all health services provided by doctors to prevent the risk of legal complaints by patients (or their relatives) for malpractice. Hypothetically including all the clinical activities (superfluous visits and/or tests) that doctors carry out for fear of legal disputes beyond the standard treatments suggested by their professional skills, the additional services induced by defensive medicine tend to generate an artificial increase of health care costs.

77 *Loi relative aux droits des malades et à la qualité du système de santé*, n° 2002-303 4 mars 2002.

78 *Loi relative à l'indemnisation des dommages résultant de soins de santé*, 31 mars 2010.

ISS are not ‘made subject to stricter requirements than those provided for by the substantive law in force in the Member State in which the service provider is established.’⁷⁹

According to the Commission,⁸⁰ in contractual relationships between health-care professionals (professional-to-professional relationships) the applicable law may be identified through a choice-of-law agreement entered by the parties (art 3 Rome I Regulation). Failing that, the law of the Member State where the service provider has his or her habitual residence will apply (art 4 (1)(b)), intended as his or her principal place of business (art 19 (1)).

The Commission does not mention it, but it could also be thought of using the exception clause by invoking the ubiquity of the e-Health service and the closest connection with the patient’s country of residence:⁸¹ this solution would make it possible to avoid possible conflicts of the law of the place of business of the service provider with the law of the patient’s habitual residence, and to have to verify the presence of mandatory rules in this last law, pursuant to art 9 (such as, for example, rules that prohibit the provision of certain services exclusively by telemedicine, in the diagnosis and/or treatment phase, with the consequence that the provision of those services would be unlawful pursuant to art 9(3)).

On the other hand, in the case of a relationship between doctor and patient, the Commission considers the protective rules for consumers applicable under art 6 Rome I Regulation which recalls the law of the country where the consumer has his habitual residence (art 6(1) Rome I Regulation), however leaving the parties the possibility to choose the applicable law, provided that such a choice hasn’t the result of depriving the consumer of the protection afforded

79 Joined Cases C–509/09 and C–161/10 *eDate Advertising GmbH and Others v X and Société MGN LIMITED* [2011] ECR 2011 I-10269, para 67. Ever since *eDate and Martinez* (ibid paras 53–68), the ECJ made clear that the so-called ‘country of origin’ or ‘internal market’ principle enshrined in art 3 eCommerce Directive, although not laying down a conflict-of-law rule, limits the reach of the applicable law determined by the pertinent conflict-of-law rules of the EU Member States. In other words, the ‘country of origin’ principle operates as a substantive corrective requiring the Member States not impose upon ISS providers, by virtue of the law deemed applicable pursuant to the relevant conflict-of-law rules, more stringent regulatory standards than those provided for by the law of the Member State of establishment of the ISS. This substantive corrective applies within the eCommerce Directive’s ‘coordinated field’ (art 2(h)), that clearly encompasses the rules on civil liability; in literature eg Tobias Lutz, ‘Internet Cases in EU Private International Law – Developing a Coherent Approach’ (2017) 66 ICLQ 689; Tobias Lutz (n 70) 21; Pedro De Miguel Asensio, *Conflict of Laws and the Internet* (Edward Elgar Publishing 2021) 74–78.

80 Commission (n 24), 26ff.

81 Thus Jan D. Lüttringhaus (n 27) 323, which recalls the US practice based on the method of the ‘most significant relationship’; see Megan Cloud, ‘Robots Are Coming: A Discussion of Choice-of-Law Issues and Outcomes in Telesurgical Malpractice’ (2019) 6 Texas A&M L R 707.

to him by provisions that cannot be derogated from by agreement by virtue of the law of the country where the consumer has his habitual residence (art 6(2) Rome I Regulation). However, if the healthcare professional does not direct his activities to the Member State where the patient has his habitual residence, the general rules that recall the law chosen by the parties are applicable (on the basis of art 6(3)) or, failing that, the law of the country where the trader has his principal place of business (arts 3 and 4(1)(b)).

Finally, in a non-contractual relationship, unless the parties have chosen the applicable law (according to art 14 Rome II Regulation), the law of the country in which the damage occurs – irrespective of the country in which the event rise giving to the damage occurred, and of the country in which the indirect consequences of that event occur – is applicable (art 4(1)): ‘(h)owever, where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply’ (art 4 (2)). It should be noted that art 17 (‘Rules of safety and conduct’) paves the way for the application of the good professional standards⁸² of the place where the eHealth provider operates (*lex loci damni*). Finally, the scope of the applicable insurance contract or of the insurance regime with regard to cross-border situations will come into play.

The Commission does not mention the possible intervention of overriding mandatory rules of the forum (arts 9 Rome I and 16 Rome II Regulations),⁸³ of rules of safety and conduct in force at the place of the event giving rise to the liability (art 17 Rome II) and of public policy exception (arts 21 Rome I and 26 Rome II Regulations). But above all the Commission solves the question scholastically, neglecting the problems of qualification already pointed out with regard to jurisdiction. Regulations Rome I and II also do not solve the problem of the combination of both contractual and non-contractual liability. In this regard, in my opinion, the secondary connection envisaged by art 4(3) Rome II, which – after providing for the exceptional application of the law of the country with which, from all the circumstances of the case, the tort/delict is manifestly more closely connected – specifies that ‘(a) manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question’. This solution is particularly interesting for Member States whose legal system allows both contractual and non-contractual obligations

82 Art 4 Oviedo Convention (n 27): ‘Any intervention in the health field (...) must be carried out in accordance with relevant professional obligations and standards.’

83 On the possible relevance of the prohibition of remote processing provided for by the rules of the Medical Order, as overriding mandatory provisions under art 9 Rome I Regulation and/or rules of safety and conduct under art 17 Rome II Regulation, see – with reference to Germany – Andreas Spickhoff, ‘Rechtsfragen der grenzüberschreitenden Fernbehandlung’ (2018) 36 *Medizinrecht* 535.

between the same parties. 'By having the same law apply to all their relationships, this solution respects the parties' legitimate expectations and meets the need for sound administration of justice. On a more technical level, it means that the consequences of the fact that one and the same relationship may be covered by the law of contract in one Member State and the law of tort/delict in another can be mitigated'.⁸⁴ Thus, the non-contractual liability of healthcare professionals could be absorbed by the *lex contractus*, which would thus govern both contractual and non-contractual liability.

6. Concluding remarks

Telemedicine and eHealth services raise a wide range of complex substantive legal issues. These complexities are further exacerbated by the ever-changing shape of the digital environment, last but not least in the light of the rapid spread of AI-based systems and related technologies. The challenging regulatory choices needed to adequately cope with the digital transformation of the healthcare sector become tremendously more pronounced when the provision of healthcare services based on ICTs bridges national borders. Private international law is generally understood as a discipline aimed at enabling the interoperability of diverse (unharmonised) legal orders. In recent years the EU legislator has undoubtedly presented itself as a particularly active player in harmonising the Member States' substantive regimes on civil liability, last but not least in the light of 2024 package of rules aimed at adapting liability rules to the AI-based digital ecosystems. Yet, the path of deepening substantive harmonisation is deeply unlikely to result in complete EU-wide standardisation of national civil law regimes, primarily because of structural limitations of the EU legal order. Against this background and despite their technologically neutral approach, the general instruments of EU private international law have, for the time being, proved to be rather resilient and relatively fit for accommodating diverse legal orders in the digital age. Yet, their interaction with cross-border telemedicine and eHealth services remains to some extent complex and uncertain, last but not least in the light of the uncertain characterization of medical liability. If the widespread deployment of eHealth is truly meant to be achieved within the EU, consistently with the position seminally expressed by the European Commission back in the 2010 Digital Agenda for Europe, private international law issues of eHealth should not be neglected. Quite on the contrary, delivering sound guidance on how the general instruments of EU private international are meant to govern cross-border eHealth services should remain a critical priority

84 Commission, 'Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations ("Rome II")' (Communication) COM (2003) 427 final, sub art 3 'General exception and secondary connection'.

to achieve interoperability of eHealth in Europe to the benefit of EU citizens, the EU Member States' healthcare sectors and medical research.

Legal Challenges for the Regulation of the European Health Data Space

Luz M. Martínez Velencoso

University of Valencia, Spain

ORCID 0000-0001-8934-3859

DOI: 10.54103/milanoup.215.c459

Abstract

In the present context of the so-called ‘Digital Society’, an important process of legislative reform is taking place inside the European Union. In areas such as the digital transformation of the health sector, these actions have a considerable impact on traditional legal concepts and categories such as privacy or informed consent. This is especially relevant in the realm of health science research in the context of Big Data. The nature of this type of research projects requires a new model of consent, which is called broad consent. The legislator faces the challenge of having to respect, on the one hand, the balance between the possibility of obtaining consent in a simple and feasible way, and on the other, the need to provide data subjects the necessary information and control over their sphere of privacy. Likewise, a formula must be found that protects individuals, but does not unduly hinder progress in biomedical research. This issue requires an assessment from both an ethical and a legal perspective. Here comes into play the role of Research Ethics Committees that is reinforced by these new legislative measures, so that the concept of data ethics is coined. In the drafting of this work, my experience as a member of the Research Ethics Committee of the University of Valencia has been fundamental.

Keywords

Informed Consent, Data Protection, Big Data, Health Research, eHealth

1. Introduction

Undoubtedly, new technologies are called upon to play an important role in the advancement of medicine, especially in what is known as personalized medicine, whose aim is for people to receive the kind of treatment most appropriate

to their specific conditions, considering their genetic makeup and other medical characteristics. For these therapies to be widely implemented, it is necessary to previously carry out research that requires a huge amount of health data, but also genetic data, which fall within the special categories of personal data, according to the terminology of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).¹ Therefore, we are faced with two conflicting interests, on the one hand, the necessary scientific progress, and on the other, the protection of the privacy of the subjects. GDPR uses instruments such as anonymization and pseudonymization of data with certain guarantees to harmonize these two positions.

Furthermore, the Data Governance Act introduces the concept of ‘data altruism’ aimed at facilitating non-profit data sharing, by fixing incentives for particulars in a trust environment.² This Regulation is part of the Commission’s plan of establishing a single European Data Space. Particularly the Proposal for a Regulation on the European Health Data Space³ “will address health-specific challenges to electronic health data access and sharing, is one of the priorities of the European Commission in the area of health and will be an integral part of building a European Health Union’.⁴

2. ‘eHealth’: the digital transformation of the health sector in the European Union

The need to regulate research in Genomics and the so-called Biobanks has had a great impact on traditional legal concepts and categories such as personal data protection or informed consent. In relation to the first question, the social function of data is valued, as an element that can contribute to the advancement of scientific knowledge. For the minimization of risks concerning privacy the concept of anonymized or pseudonymized data arises. Such data no longer identifies the subject and can be used for research in Big Data environment with guarantees. On the second issue, the subject’s consent to participate in a

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L119/1.

2 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.

3 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space’, COM (2022) 197 final.

4 Explanatory memorandum ‘Reasons for and objectives of the proposal’.

research project, as it was shaped in the European Bioethics Convention, needs to be reformulated so that it is best suited for these new forms of research, as it will be discussed in more detail below.⁵

The European Union is issuing new rules aimed at the new regulation of the digital society. One of the issues to which special attention is paid is what is called ‘eHealth’ (eHealth Action Plan 2012-2020),⁶ which is conceived as preventive, predictive, personalized, participatory and populational medicine and through technological devices developed for therapeutic or care purposes.⁷ Truly, this is going to mean a change in the model of healthcare as we know it today.

As previously mentioned, the implementation of this new health system requires prior research work, where the so-called Big Data in health is bound to play an important role. In this form of research, personal data is essentially valuable. Much of this data comes from what is called the ‘Internet of Bodies’, a subcategory within ‘Internet of Things’ that facilitates practices such as monitoring people’s health data. Among the advantages of these technologies, it can be mentioned that the treatment of this huge amount of data will allow scientific progress in the field of Genetic Medicine, since it will make possible to understand the interaction between genetics and the environment of the person to contribute to the discovery of new diagnostics and therapies. However, this technology is not exempt from risks, such as possible discrimination of the person due to his or her genetics, which is prohibited by Constitutional texts and International Treaties on the matter, as well as possible violations of privacy, since although pseudonymization or anonymization techniques exist, re-identification is sometimes possible. This last question is especially serious, since genetic data and health data are highly sensitive data, subject to a higher level of protection in the corresponding personal data protection regulations.

Returning to the topic of the so called 5P Medicine, one of the main objectives of the ‘eHealth Action Plan 2012-2020’ of the European Union is to obtain better data to promote research, disease prevention, and personalized health care.⁸

5 In relation to this question cf Barbara J Evans, ‘Big Data and Individual Autonomy in a Crowd’, I. Glenn Cohen and others (eds), *Big Data, Health Law, and Bioethics* (CUP 2018) 19, 26. In the context of Big Data, the traditional norms on informed consent are not adequate for the main purpose for which they were designed: to empower the individual to protect themselves against research-related risks.

6 European Parliament, ‘Resolution on the eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century (2013/2061(INI))’ [2016] OJ C482/14.

7 Paragraph 6 of Art. XXIII Carta de Derechos Digitales 2021.

8 Virginia Sanchini and Luca Marelli, ‘Data protection and ethical issues in European P5 eHealth’ in Gabriella Pravettoni and Stefano Triberti (eds), *P5 eHealth: An Agenda for the Health Technologies of the Future* (Springer 2020) 173.

In the same vein, measures must be adopted that allow the assemblage of genomic data and other health data, guaranteeing full compliance with data protection legislation and the corresponding respect for ethical principles. The European Commission underlines the advantages of a coordinated European action in this field by ‘making it possible to tackle major health challenges such as cancer or brain disease, epidemics of infectious disease, or rare disease’.⁹ Furthermore, the intention is to fix coordination between authorities across the EU to implement the secure exchange of genomic and other health data to advance research and implement personalised medicine. ‘This should be based on a transparent system of governance, with the aim of linking national and regional banks of ‘-omics’ data, biobanks and other registries across the EU’.¹⁰

The expected result of all this is the conjunction of information from molecular profiling, diagnostic imaging, environmental and lifestyle data, microbiological genomics and environmental data as well as links to electronic health records.

The purpose is to implement predictive methods regarding digital patients with the support of high-performance computing, data analytics and artificial intelligence.

3. Towards the European Health Data Space: legal instruments

3.1. The Regulation (EU) 2016/679

In this task aimed at achieving personalized and predictive medicine, the GDPR plays an important role as a legal instrument. The Regulation allows the promotion of research and provides an opportunity to strike a fair balance between the protection of individual rights and scientific progress.

In recital n 34 a concept of genetic data is provided as ‘personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained’. Likewise, in Recital 35 among the personal data related to health, it must be included all data related to the state of health of the subject which provide information about the state of physical or mental health, past, present, or future, as well as those obtained from biological

9 Commission, ‘Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society’, COM (2018) 233 final, 7.

10 *ibid* 8.

samples. This interpretation is in line with the case law of the European Court of Human Rights, which in *S. and Marper v UK* ruled that the cell samples constitute personal data (in the opinion of the Court, the analysis of the biological sample of the plaintiff implies an interference with the right to privacy due to the potential risks that such analysis could derive from).¹¹

Health data and genetic data of people fall within the special categories of data of art 9 GDPR. However, there is a paradigm shift in the understanding of health data, which is called upon to achieve a social function.

In the first place, according to recital n 4 GDPR: ‘The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity’.

Secondly, in recital n 53 GDPR reference is made to health data and genetic data as special categories of personal data ‘which merit higher protection’ and that ‘should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems’. However, as it continues to be pointed out, these data may also be processed for ‘archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health’.

How is it possible to harmonize individual interest and social interest in this balanced analysis? The answer must be found in art 89 GDPR that establishes a series of guarantees and exceptions applicable to the processing of data for

11 *S. and Marper v UK* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2004, para 73, stating: ‘Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (see Amann cited above, § 69)’. Among scholars cf Dara Hallinan and Paul De Hert, ‘Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research’ in Brent Daniel Mittelstadt and Luciano Floridi (eds), *The Ethics of Biomedical Big Data* (Springer 2016) 119.

scientific research purposes.¹² Among them it is mentioned that ‘technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation’. Likewise, said measures ‘may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner’. It is about respecting the principle of data minimization, which according to art 5(1)(c) personal data shall be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimization”)’.

Thus, the further processing of personal data will be carried out when the data controller has evaluated the feasibility of fulfilling these purposes through data processing that does not allow the identification of interested parties, such as pseudonymization.¹³

In addition, it is possible to establish exceptions to the rights of access, rectification, deletion, limitation and opposition to the processing and portability of the personal data of the subject, when they may make it impossible or seriously hinder the achievement of the scientific and when those exceptions are necessary to achieve those purposes.

3.1.1. Broad consent model for health research and research for public interest in the realm of Big Data

Another useful instrument mentioned above is the broad consent model referred to in recital n 33 GDPR. Due to the new ways of research in the context of Big Data, it is often not possible to ‘fully identify the purpose of personal data processing for scientific research purposes at the time of data collection’. That is why ‘data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research’. Consequently, data subjects must be given the opportunity

12 About this issue cf Menno Mostert and others, ‘From Privacy to Data Protection in the EU: Implications for Big Data Health Research’ (2018) 25 European Journal of Health Law 43, 53. In the opinion of the authors, in the tension between scientific progress and the protection of the individual, the European Data Protection Regulation allows exceptions to certain consent requirements for the sake of scientific research, but also requires that said exceptions are subject to appropriate guarantees. In accordance with art 89, para 1, of the GDPR, technical and organizational measures must be adopted to guarantee respect for the principle of data minimization. The question of what specific safeguards should be provided by law regarding data-intensive health research remains unclear. The authors point out, among others, accountability to an independent supervisory entity, respect for the principle of transparency, allowing interested parties to invoke their rights, among others. However, the adoption of inflexible or rigid data protection measures could hinder the establishment of adequate information governance frameworks, and ethics and law must be reconciled.

13 As established in recital n 156 GDPR.

to give their consent ‘only to certain areas of research or parts of research projects to the extent allowed by the intended purpose’.

The current regulations on data protection rest on the concept of informed self-determination of the subject (‘informational self-determination’), that is, in the ability of data subjects to take control over the assignment or use that will be given of their personal data based on their free and informed consent (‘privacy self-management’). However, given the nature of research projects in the context of Big Data, the traditional informed consent model may be impractical. Art 60 of the Spanish Act 14/2007 on Biomedical Research (Biomedical Research Spanish Act) establishes that consent will be specifically obtained for a specific investigation.¹⁴ However, the ‘broad consent’ models, to which the mentioned recital n 33 refers, have the problem that people are often no longer capable of making significant decisions about the use of their personal data as a consequence of the complexity of health research in the context of Big Data. In this environment, a balance cannot always be struck between obtaining consent in a simple and feasible way, and providing data subjects with sufficient information and control, when personal data is to be linked to others, reused, and analysed in future unspecified research projects.¹⁵

The general rule, according to art 9 GDPR, is that it is not possible to process genetic data, data related to the health of the person, among others within the special categories of data. However, this limitation will not apply when the interested party has given ‘explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’ (for example, there are States where the processing of genetic data by insurance companies for risk assessment in life or health insurance is prohibited).¹⁶

14 Ley 14/2007 Investigación biomédica.

15 cf Markus Christen and others, ‘On the Compatibility of Big Data Driven Research and Informed Consent: The Example of the Human Brain Project’ in Brent Daniel Mittelstadt and Luciano Floridi (eds), *The Ethics of Biomedical Big Data* (Springer 2016) 199, 201. In the opinion of the authors, any form of informed consent is embedded in an “information framework” that indicates the general context in which the data is generated, what type of data is actually obtained, and, although not exhaustively and in rather general terms, what kind of results could be expected from the analysis of the data.

16 This is the case, for example, of Belgium: in this country the Loi du 4 Avril 2014 relative aux assurances specifically regulates the use of genetic information by insurance companies. Art 58 establishes that genetic data cannot be communicated to insurance companies for the purposes of risk assessment. Likewise, as regulated in art 61(3), the medical examinations necessary for the conclusion and execution of the contract can only be based on the current state of health of the insured person and not on genetic research techniques to predict the future state of health. Therefore, even if the subject’s consent was given, insurers would not be able to use the person’s genetic information for the purposes of risk assessment within the scope of the insurance contract.

This consent can be broad consent within the meaning of recital 33 GDPR when the processing of genetic or health data is for research purposes.¹⁷ As an argument in favour of this new model, it is cited that due to the complexity and dynamism of modern biomedical research, research participants may not be aware of all the current implications derived from the provision of their consent. In addition, it is often not possible to obtain renewed informed consent because it is usually not possible to find the subjects participating in the research (for example, because they have died). At the same time, maintaining a record of contact data would represent a high cost for any project, and could even generate new risks in the protection of privacy due to possible unauthorized access to this information.

The European Data Protection Board (EDPB) has explained that although recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research, “it should be noted that recital 33 does not disapply the obligations with regard to the requirement of specific consent”.¹⁸

The GDPR establishes other legal basis, other than consent, that legitimize the processing of genetic and health data. For instance, substantial public interest (art 9(2)(g)), preventive or occupational medicine, for the assessment of

17 Aaro Tupasela and Sandra Liede, ‘State Responsibility and Accountability in Managing Big Data in Biobank Research: Tensions and Challenges in the Right of Access to Data’ in Brent Daniel Mittelstadt and Luciano Floridi (eds), *The Ethics of Biomedical Big Data* (Springer 2016) 257, 263. Broad consent is understood to mean that samples and associated data may be collected for a wide range of future research purposes by using a general description of the intended research object. The specification is produced by a description of the research area which, in the field of biobanks, can be quite broad. It has been warned, however, that the regulations on data protection must be respected, which is made possible by coding the samples that are delivered to the researchers detached from the personal data of the source subject. Also, as a counterbalancing measure to this broad consent, and in addition to extensive supervision by authorities, individuals have in turn been granted extensive control over the use of their samples and data.

18 EDPB Opinion Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020, 30–31: “This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level. The notion of scientific research “may not be stretched beyond its common meaning” and understands “scientific research” in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice’. Furthermore, ‘the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes “shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject.” Data minimization, anonymisation and data security are mentioned as possible safeguards. Anonymisation is the preferred solution as soon as the purpose of the research can be achieved without the processing of personal data’.

the working capacity of the employee, medical diagnosis, provision of health or social care (art 9(2)(h)), public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical device (art 9(2)(i)). Finally, archiving purposes in the public interest, scientific or historical research purposes or statistical purpose (art 9(2)(j)).

Returning to consent as the cause that legitimizes the processing of data, initially, the Biomedical Research Act – collecting the broad lines existing up to this moment in the field of bioethics, especially the Council of Europe Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (‘Oviedo Convention’)¹⁹ – regulates in art 60 consent requirements, firstly, the consent for the use of the biological sample in research must be granted for a specific investigation. However, as established in para 2, the sample may be used for other lines of research related to the one initially proposed if so provided for in the specific consent. Otherwise, the source subject must be asked for a new consent.²⁰

Accordingly, in the ‘Report of the UNESCO International Bioethics Committee issued on 15 September 2017 on Big Data and Health’,²¹ in para 59 the Committee understands that in the event that an investigation is intended to be carried out is outside the range of the broad consent that was obtained for the use of these data, a specific consent is necessary for the subsequent treatment of these. This is an essential principle to guarantee the confidentiality and privacy of data. So far there is nothing new with respect to what is established in the mentioned art 60 of the Biomedical Research Spanish Act. However, the possibility of a secondary use of the data that could be ethically admissible without a new informed consent is admitted below, provided that all the following requirements are met: a) adequate legal basis; b) evaluation by the Research Ethics Committee; c) adequate technical procedures to prevent researchers and third parties from accessing personal data, such as pseudonymization; d) the overriding public interest in this health research; e) infeasibility of obtaining a

19 Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, 4 April 1997, ETS 164.

20 In the Basque Country Superior Court, 14 June 2017 (JUR 2017, 232851) the use of biological samples from the patient without their consent to carry out research activity is considered a very serious infringement of the data protection regulations. In this case, the data were used for different purposes from the studies that motivated the collection of biological samples and that were initially consented to. The patient had given his consent for the use of his biological samples in the ‘EM Molecular Study’ and later they were used in other lines of research, particularly in a thesis and in a study published in a scientific journal. This interpretation is in line with art 60(2) of the Biomedical Research Act.

21 Full text at <<https://unesdoc.unesco.org/ark:/48223/pf0000248724>> accessed 30 May 2024.

new consent; f) the data must have been collected in compliance with ethical and legal requirements.

This was already provided for in art 58(2) of the Biomedical Research Spanish Act, as an exception to the general rule of art 60. According to art 58(2), the ‘consent of the subject will always be necessary when it is intended to use biological samples obtained for a different purpose for biomedical research purposes’ (for example, for healthcare purposes), regardless of whether they were object of anonymization. However, ‘exceptionally, codified or identified samples may be processed for biomedical research purposes without the consent of the subject, when obtaining the consent is not possible or represents an unreasonable effort within the meaning of art 3(i) of this Act. In these cases, the favourable opinion of the corresponding Research Ethics Committee will be required, which must take into account, as a minimum, the following requirements: a) That it is an investigation of general interest; b) That the research is carried out by the same institution that requested the consent to obtain the samples; c) That the research is less effective or is not possible without the identifying data of the source subject; d) That there is no express objection of the subject; e) That the confidentiality of personal data is guaranteed’.

According to the Spanish Data Protection Agency, this non-restrictive interpretation should be considered by Research Ethics Committees in cases in which they authorize the treatment of codified samples, without consent when it is not possible to obtain it, in accordance with art 58(2) of the Biomedical Research Spanish Act.²²

The secondary use of data that was obtained for a specific purpose with the prior consent of the subject for a different purpose (for example, they were obtained for healthcare purposes, and it is intended to use them in research) requires an assessment from both an ethical and a legal perspective. This proportionality test can be carried out, on a case-by-case basis, by an independent body such as the Research Ethics Committee (whose role is reinforced in Additional Disposition 17th of the Spanish Act 3/2018 on Personal Data Protection).²³

In the transposition of the European Data Protection Regulation into Spanish law, these issues have been regulated in Additional Disposition 17th of the Spanish Act 3/2018, in lett (b) of which even allows avoiding the consent of the interested party to carry out scientific studies in situations of exceptional relevance and seriousness for public health by health authorities and public institutions with competences in public health surveillance. This implies the materialization of the legal bases of letts (g), and (i) of art 9(2) GDPR, referred

22 Report of the Spanish Data Protection Agency on the incidence that the full application of the Regulations could produce in the field of biomedical research as of 25 May 25 2018, as well as the approval of a new Organic Act on Data Protection (Report 073667/2018) 8.

23 Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

above. In this case, these are studies framed within the strict sphere of public authorities.

Likewise, lett (d) establishes that the use of pseudonymized personal data for health research purposes and particularly biomedical research, is considered lawful. For this, a technical and functional separation will be required between the research team and those who carry out the pseudonymization and keep the information that makes re-identification possible. In addition, it is specified that the pseudonymized data is only accessible to the research team when there is an express commitment to confidentiality and not to carry out any re-identification activity and when specific security measures are adopted to prevent re-identification and access by unauthorized third parties. Re-identification will be possible when the existence of a real and specific danger to the safety or health of a person or group of people is appreciated, or a serious threat to their rights or when it is necessary to guarantee adequate health care.

In this other case, research of interest to public health would be included, which is carried out by research groups in both the public and private spheres,²⁴ without the need for a new consent, with pseudonymization of the data and with a report from a Research Ethics Committee (Additional Disposition 17th lett (d)).

Furthermore, lett (c) Additional Disposition 17th considers the reuse of personal data for health and biomedical research purposes lawful and compatible when, having obtained consent for a specific purpose, the data is used for purposes or research areas related to the initial research project.

To comply with the requirement of adequate guarantees of art 89(1) GDPR the Spanish Act articulates the following safeguards:

a) The publication of the information required by art 13 of the GDPR by the data controller on the corporate website of the research centre.

b) Notification by electronic means to those affected informing of the existence of said information.

c) A favourable report of the Research Ethics Committee.

In addition, in lett (f) Additional Disposition 17th of the Spanish Act 3/2018 on Personal Data Protection establishes certain requirements that biomedical research projects must meet, among them an impact assessment must be carried out. The so-called impact assessment should consider how the rights and freedoms of the subjects are affected, the measures aimed at guaranteeing the

24 As stated in recital n 159 of GDPR: 'Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research'.

security of the information and, where appropriate, the quality of the pseudonymization or anonymization instruments that are adopted.²⁵

As revealed in the ‘Report of the Bioethics Committee of Spain on the Ethical-Legal requirements in Research with Health data and Biological Samples in the Framework of the Covid-19 pandemic of 28 April 2020’²⁶ the secondary use of health data for health research in the realm of the public interest requires a prior weighted analysis of the interests at stake.

As noted in this report, the classic model of the informed consent of the subject comes from the main international charters in the field of Bioethics such as the Nuremberg Code or the Declaration of Helsinki.²⁷ In these investigations the physical integrity and dignity of the person were at risk. In the current context of Big Data, research deals with information (‘informational research’), referring, indeed, to a person, but the interest at stake is different, it is about preserving his or her privacy.²⁸

As mentioned, in Additional Disposition 17th of the Spanish Act 3/2018 on Personal Data Protection, specifically in its second section, in the realm of health research, it’s a question of weighing up the great benefits that it brings to society without ignoring the fundamental right to the protection of personal data. Therefore, this regulation represents a necessary paradigm shift for a new model of health research.

25 Cf Ricard Martínez Martínez, ‘Big data, investigación en salud y protección de datos personales. ¿Un falso debate?’ (2017) 62 Revista Valenciana d’Estudis Autònoms 235, 269.

26 Full text at <<https://comitedebioetica.es/>> accessed 30 May 2024.

27 ‘Permissible Medical Experiments’. Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10. Nuremberg October 1946 – April 1949, Washington. U.S. Government Printing Office (n.d.), vol. 2, 181–182.

Ethical Principles for Medical Research Involving Human Subjects Adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964.

On this topic see Federico De Montalvo Jääskeläinen, ‘Uso secundario de los datos de salud en el marco del Big Data: ¿Hacia un cambio jurídico del “Paradigma Helsinki?”’ in Miguel Angel Recuerda Girela (ed), *Tecnologías disruptivas: regulando el futuro* (Aranzadi Thomson Reuters 2019) 423.

28 However, the European Data Protection Board in ‘Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak’, adopted on 21 April 2020, 13 mentions that: ‘in certain situations, in particular where transfers are performed by private entities for the purpose of medical research aiming at fighting the COVID-19 pandemic, such transfers of personal data could alternatively take place on the basis of the explicit consent of the data subjects. Public authorities and private entities may, under the current pandemic context, when it is not possible to rely on an adequacy decision pursuant to Article 45 (3) or on appropriate safeguards pursuant to Article 46, rely upon the applicable derogations mentioned above, mainly as a temporary measure due to the urgency of the medical situation globally. Indeed, if the nature of the COVID-19 crisis may justify the use of the applicable derogations for initial transfers carried out for the purpose of research in this context, repetitive transfers of data to third countries part of a long-lasting research project in this regard would need to be framed with appropriate safeguards in accordance with Article 46 GDPR’.

3.2. The Data Governance Act

The Data Governance Act introduces the concept of “data altruism” aimed at facilitating non-profit data sharing, by fixing incentives for particulars in a trust environment.²⁹ This Regulation is part of the Commission’s plan of establishing a single European Data Space.

As stated in art 2(10): “data sharing” means the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licenses subject to a fee or free of charge’. According to recital n 45 ‘There is a strong potential for objectives of general interest in the use of data made available voluntarily by data subjects on the basis of their informed consent or, where it concerns non-personal data, made available by data holders. Such objectives would include healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, or public policy making. Support to scientific research should also be considered to be an objective of general interest’.

Consent still has a great role as a legitimate basis for the data to be processed, in art 2(5) ‘consent’ means consent as defined in art 4 (11) of Regulation (EU) 2016/679. It is distinguished between data and non-personal data.³⁰ Consequently, data altruism would rely on consent.³¹

Furthermore, it is foreseen in the Data Governance Act a so-called “data altruism consent”, a new model of consent for making data available for reuse,

29 Corina Kruesz and Felix Zopf, ‘The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU’ (2021) 7 *European Data Protection Law Review* 569.

30 The Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59 provides a negative definition in art 3(1) as “data other than personal data”. The non-personal nature of such data might include a wide range of information: machine-generated data and commercial data, whether they have never been personal (not relating to an identified or identifiable person), or later anonymized.

31 Recital n 50: ‘Typically, data altruism would rely on consent of data subjects within the meaning of Article 6(1), point (a), and Article 9(2), point (a), of Regulation (EU) 2016/679 that should be in compliance with requirements for lawful consent in accordance with Articles 7 and 8 of that Regulation’.

Also, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 10 March 2021, 39: ‘underline that one of the main objectives of the GDPR is to ensure that the data subject keeps control over her or his personal data. In this context, the EDPB and EDPS underline that all requirements related to the consent, as set in the GDPR, need to be fulfilled’. There must be compatibility of data altruism consent with the consent requirement under the GDPR.

including by particulars for altruistic grounds. A common European data altruism consent form will be developed to reduce the costs of collecting consent and to facilitate portability of the data (in case data to be made available is not kept by the individual).³²

Therefore, an altruism consent form has to be developed for boosting a trustful environment for particulars to consent the processing of their data, particularly in the realm of scientific research.³³

Additionally, Chapter IV regulates data altruism (data voluntarily made available by individuals or companies for the common good). It establishes the possibility for organisations engaging in data altruism to register as a 'Data Altruism Organisation recognised in the EU' in order to increase trust in their operations.

Secondary use of data is defined in art 2(2): "re-use" means the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks'. Conditions for re-use are established in art 5 of the Data Governance Act.³⁴ Furthermore, public

32 Recital n 52: 'To promote trust and bring additional legal certainty and user-friendliness to the process of granting and withdrawing consent, in particular in the context of scientific research and statistical use of data made available on an altruistic basis, a European data altruism consent form should be developed and used in the context of altruistic data sharing. Such a form should contribute to additional transparency for data subjects that their data will be accessed and used in accordance with their consent and also in full compliance with the data protection rules. It should also facilitate the granting and withdrawing of consent and be used to streamline data altruism carried out by undertakings and provide a mechanism allowing such undertakings to withdraw their permission to use the data'.

33 Recital n 52: 'To promote trust and bring additional legal certainty and user-friendliness to the process of granting and withdrawing consent, in particular in the context of scientific research and statistical use of data made available on an altruistic basis, a European data altruism consent form should be developed and used in the context of altruistic data sharing. Such a form should contribute to additional transparency for data subjects that their data will be accessed and used in accordance with their consent and also in full compliance with the data protection rules'.

34 Among other requirements it is established that conditions for re-use 'shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed.' Furthermore, these conditions 'shall not be used to restrict competition'.

To guarantee the preservation of the protected nature of data, data have to be '(i) anonymised, in the case of personal data; and (ii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights'. Also, access and re-use of the data should be done 'within a secure processing environment that is provided or controlled by the public sector body' and 'within the physical premises in which the secure processing environment is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties'.

sector bodies which allow re-use of data may charge fees for allowing the re-use of such data (art 6(1)).

In the realm of data altruism, if the data processed are personal data, GDPR has to be applied additionally to the Data Governance Act.³⁵ Specifically, data subject rights provided by the GDPR are applicable in the context of the Data Governance Act.

Subsequently, organisations that process data altruistically should be considered controllers (co-controllers) insofar as they will determine the purposes of the processing of personal data, for example the framework conditions for a specific research project.³⁶

The GDPR in art 89 contains also special rules in data processing for scientific research purposes which can collide with the norms of the Data Governance Act, particularly art 21 establishes specific requirements to safeguard rights and interests of data subjects and data holders with regard to their data. First of all, some duties to inform should be accomplished, among others the data subject should be informed about the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which personal data is to be processed, and for which it permits the processing of his or her data. Furthermore, according to para 2, the data altruism organisation is not entitled to use the data for other objectives than those of general interest for which the data subject or data holder allows the processing. Otherwise, the GDPR in art 89(1) accepts further processing of personal data in the public interest, scientific or historical research purposes or statistical purposes. The general rule appears to be less restrictive than the more special one.

Furthermore, to ensure the safe processing of personal data additional measures are to be considered, and again the role of the ethics committee is highlighted.³⁷

35 Proof of this coordination is that the Data Governance Act mentions the broad consent in the realm of scientific research in recital n 50: 'In accordance with the GDPR, scientific research purposes could be supported by consent to certain areas of scientific research where in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects'.

36 In this vein also art 51 of the Proposal for a Regulation on the European Health Data Space: '1. The health data access bodies and the data users, including Union institutions, bodies, offices and agencies, shall be deemed joint controllers of electronic health data processed in accordance with data permit'.

37 Recital n 46: 'Further safeguards should include making it possible to process relevant data within a secure processing environment operated by the recognised data altruism organisations, oversight mechanisms such as ethics councils or boards, including representatives from civil society to ensure that the data controller maintains high standards of scientific ethics and protection of fundamental rights, effective and clearly communicated technical means to withdraw or modify consent at any moment, on the basis of the information obligations of data processors under Regulation (EU) 2016/679, as well as means for data subjects to stay informed about the use of data they made available'.

In conclusion, the concept of general interest or common good seems to be very important for the use of data on altruistic grounds.³⁸ One of the objectives of general interest is to support scientific research as mentioned in the Recitals of the Data Governance Act. Still this concept has to be clarified, in the preamble of the GDPR has been included as an example of scientific research ‘privately funded research’. However, apart from the nature of funding, other circumstances of the research should be taken into consideration, as the population under study, types of benefit sharing or equitable access to research databases.³⁹

3.3. The Proposal for a Regulation on the European Health Data Space

This norm is aimed at providing for rules, common standards and practices, infrastructures, and a governance framework for the primary and secondary use of electronic health data (art 1). Among the measures it is included the creation of ‘a mandatory cross-border infrastructure for the secondary use of electronic health data’ (art 2(e)).

It is fixed a list of categories of electronic data available for secondary use: ‘(a) EHRs (electronic health record systems); (b) data impacting on health, including social, environmental behavioural determinants of health; (c) relevant pathogen genomic data, impacting on human health; (...); (e) human genetic, genomic data (art 33(1))’.

Furthermore, a list of purposes for which electronic health data can be processed for secondary use is established (art 34): ‘(a) activities for reasons of public interest in the area of public and occupational health, such as protection

38 About the concept of public interest, EDPS Preliminary Opinion on Scientific Research, 2020 adopted on 6 January 2020, 23: ‘necessity and the public interest imply a “pressing social need” as opposed to largely private or commercial advantages’. Furthermore, the important role of ethics committee is highlighted (25): ‘Data protection authorities and data protection officers increasingly engage with ethical questions in the development and deployment of digital technologies. They should engage more closely with ethical review boards. Genetic research in particular has implications not only for the subject of the DNA tests but others in his or her family or with shared characteristics in this and future generations. Independent ethical committees could support the understanding of which activities qualify as genuine research and define the ethical standards referred to in the GDPR. Ethics committees can play a meaningful role in ensuring that the respect of human rights, including right to data protection, is embedded in the research project from the early planning stage. They are likely to continue to play an important role in ensuring that research projects are designed from the start with data protection principles in mind.’

39 Marieke Bak and others, ‘You Can’t Have AI Both Ways: Balancing Health Data Privacy and Access Fairly’ (2022) 13 *Frontiers in Genetics* 1, 5.

against serious cross-border threats to health, public health surveillance or ensuring high levels of quality and safety of healthcare and of medicinal products or medical devices; (b) to support public sector bodies or Union institutions, agencies and bodies including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates; (c) to produce national, multi-national and Union level official statistics related to health or care sectors; (d) education or teaching activities in health or care sectors; (e) scientific research related to health or care sectors; (f) development and innovation activities for products or services contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices; (g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices; (h) providing personalised healthcare consisting in assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons’.

One of the goals of this secondary use of data is the training of artificial intelligence algorithms mentioned also in the Proposal for a Regulation on artificial intelligence,⁴⁰ it is in line with the implementation of new form of medicine more sustainable.⁴¹

40 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts’ COM (2021) 206 final, recital n 45: ‘For the development of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as digital innovation hubs, testing experimentation facilities and researchers, should be able to access and use high quality datasets within their respective fields of activities which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems’.

41 cf Principle XXIII number 2 of the Spanish Digital Rights Charter: ‘Public authorities shall promote that research and technology contribute to the achievement of a preventive, predictive, personalized, participatory and population-based medicine’. Of course, there are some risks to be eluded, as mentioned in number 6 of the same principle: ‘Public authorities will promote universal access to telemedicine systems and telecare, as well as technological devices developed for therapeutic purposes or assistance in adequate conditions of connectivity. Efforts will be made to establish that access to such devices were provided free of charge by a manufacturer or supplier cannot be conditioned to the transfer to those of the patient’s personal data’.

However, some purposes are explicitly prohibited: art 35(b) considers, for instance, ‘taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums’.⁴²

For the implementation of such future Regulation, it is necessary to develop a mandatory cross-border infrastructure for secondary data use. Consequently, ‘Health Data Access Bodies’ must be established in all member States, as the governance of the EHDS is assigned to Health Data Access Bodies (arts 36–43) that can issue data licenses to access data to potential data users, provided that some procedural and material conditions are fulfilled (including purpose limitation as stated in art 44 of the Proposal Regulation). It is regulated the possibility to fix a fee, in art 42 charged by health data access bodies and single data holders for making electronic health data available for secondary use.

Scholars have highlighted that drafters of the EHDS still have a difficult task to develop, considering the existing legal complexities for the consent requirements and uncertainties regarding the concept of scientific research for the public interest.⁴³

42 According to Principle XXI number 4 of the Spanish Digital Rights Charter: ‘The development of scientific and technological research likely to have an impact on the human being must respect the dignity and guarantee respect to every person, without any discrimination, related to the integrity and other fundamental rights and freedoms with respect to the applications of biology and medicine. Likewise, research will be governed by ethical principles and scientific integrity. All this within the framework of the Spanish Constitution and the laws’.

43 Bak and others (n 39) 3.

Tele-abortion: between privacy and women's reproductive rights

Sara Dal Monico

Università Ca' Foscari Venezia, Italy

ORCID 0000-0002-5058-8688

DOI: 10.54103/milanoup.215.c460

Abstract

Women's reproductive health in general and the right to abortion in particular have been targeted and challenged in recent years world-wide in a number of countries: to name a few, first the almost entire ban on abortion in Poland 2020, then the overthrow of *Roe v. Wade* by the Supreme Court of the USA in 2022. Although in international law a right to abortion has not been expressly codified in any international binding convention, regional courts have tried to recognise the existence of such right as a corollary to other human rights such as the right to privacy and the right to be free from inhuman or degrading treatment. To overcome such challenges, in some US States and in South America, a practice has emerged drawing from the most recent developments in e-health, which is that of tele-abortion, which would allow women in need of ending an unwanted pregnancy to access the service remotely, through the abortion pill and with the supervision of a doctor through a series of online meetings. Nonetheless, resorting to such method raises a number of legal issues, which this paper aims at analysing and examine in depth from an international law perspective. Among the issues addressed by this paper, is whether tele-abortion can be considered as a means to ensure women's reproductive rights, which will be approached through an intersectional lens, as well as the close connection between tele-abortion and women's right to privacy, focusing on the safeguarding of the collection and storage of data in case of tele-abortion. In this regard, the paper will highlight the legal vacuum in international law in terms of the developments of e-health particularly, and AI in general, fields in which the international legal framework is still lagging behind.

Keywords

Women's Reproductive Health Rights; Tele-Abortion; E-Health; Right to Privacy; Right to Abortion

1. Introduction

Modern technologies and artificial intelligence (AI) can be instrumental to the enjoyment of human rights. The digitalization has brought about changes and advancements in how human rights are enjoyed also in the field of health care, as well as challenges, which international law in particular might be unequipped for. As a global phenomenon, the digitalization is an issue which international law cannot overlook, especially when it impacts human rights. The practice analysed in this contribution defined as Teleabortion is particularly relevant in this regard, since it demonstrates how advancements in technologies and artificial intelligence can be of service in delivering several human rights, such as women's right to health, women's reproductive rights and the right to autonomy.

In times where the right to abortion, although not expressly recognised at the international level as it will be recalled, has received challenges and threats from different parts of the world, such as the almost total ban on abortion in Poland,¹ as well as the recent overturn of the US Supreme Court judgment *Roe v Wade*,² the use of telemedicine also in this field should be investigated, which this contribution aims at doing. The contribution will explore first the practice of Teleabortion, then investigate its possible advantages in terms of service delivery and enjoyment of women's reproductive rights and will move onto the considerations of one of the main possible challenges to the use of AI in that field: data protection. The purpose of this contribution is therefore to explore the access and use of Teleabortion as an 'enabler' of rights – borrowing the expression from the Office of the High Commissioner for Human Rights (OHCHR), which has however used it in the context of the right to privacy in

1 Letta Tayler, 'Two Years On, Poland's Abortion Crackdowns and the Rule of Law' (Human Rights Watch, 22 October 2022) <<https://www.hrw.org/news/2022/10/22/two-years-polands-abortion-crackdowns-and-rule-law>> accessed 26 April 2023; European Parliament, 'European Parliament Resolution of 11 November 2021 on the first anniversary of the de facto abortion ban in Poland 2021/2925(RSP)' [2021] OJ C 205/44. The Resolution underlines at paragraph 1: 'its strong condemnation of the illegitimate Constitutional Tribunal's ruling of 22 October 2020 that imposes a near-total ban on abortion', stressing the illegality of an almost total criminalization of abortion.

2 *Dobbs, State Health Officer of the Mississippi Department of Health, et al v Jackson Women's Health Organization et al*, Certiorari to the United States Court of Appeals for the Fifth Circuit, [2022] USSC 597 US.

the digital age³ – in particular, women's reproductive rights and on the other hand, the possible threats deriving from it, focusing on the right to privacy and data protection. It will be pointed out that the current international law framework concerning data protection is still lacking behind especially in regards to sensitive data such as those concerning health care.

2. Abortion in international law

The central issue of this contribution is not to enquire whether a right to Teleabortion exists. This issue indeed falls under the broader notion of the right to abortion. The underlying question which needs to be addressed is whether there is a right to abortion in international law. The literature on abortion in this field is extensive, and it has been discussed under different perspectives: as a human rights issue, including the prohibition of torture and inhuman, cruel or degrading treatment and as violence against women.⁴ Nonetheless, one aspect emerges in particular: international law is lacking behind in recognising the right to abortion both at the customary and treaty law level. No international treaty or custom expressly states that a (human) right to abortion exists, hence scholars have tried to ground the legitimacy of the right to abortion within other

3 Human Rights Council, Forty-eighth session 13 September–1 October 2021, 'The right to privacy in the digital age. Report of the UN High Commissioner for Human Rights' (13 September 2021) [2021] UN Doc A/HRC/48/31.

4 On abortion and human rights, see: Joanna N. Erdman, 'Abortion in International Human Rights Law' in Sam Rowlands (ed), *Abortion Care* (CUP 2014); Joanna N. Erdman and Rebecca J Cook, 'Decriminalization of abortion – a human rights imperative' [2020] 62 *Best Practice & Research Clinical Obstetrics and Gynecology* 11, 24; Daniel Fenwick, 'The modern abortion jurisprudence under Article 8 of the European Convention on Human Rights' [2013] 12 *Medical Law International* 249, 276; Mariana Prandini Assis, Joanna N. Erdman, 'Abortion rights beyond the medico-legal paradigm' [2022] 17 *10 Global Public Health* 2235, 2250; Ronli Sifris, 'Restrictive Regulation of Abortion and the Rights to Health' [2010] 18 *Medical Law Review* 185, 212; Sara De Vido, 'Conscientious Objection and Access to Abortion in the Case *CGIL v. Italy* Decided by the European Committee of Social Rights' [2019] 47 *Hitotsubashi Journal of Law and Politics* 45, 55. On abortion and violence against women: Sara De Vido, *Violence Against Women's Health in International Law* (Manchester University Press 2020); UN Committee for the Elimination of All Forms of Discrimination against Women, 'General Recommendation No. 35 on Gender-Based Violence against Women, Updating General Recommendation No. 19' (26 July 2017) UN Doc CEDAW/C/GC/35. On abortion and cruel, inhuman or degrading treatment see: Ronli Sifris, *Reproductive Freedom, Torture and International Human Rights: Challenging the Masculinisation of Torture* (Routledge 2014); Alyson Zureick, '(En)gendering Suffering: Denial of Abortion as a Form of Cruel, Inhuman, or Degrading Treatment' [2015] 38 *Fordham International Law Journal* 99, 140; Sara Dal Monico, 'La criminalizzazione dell'aborto quale divieto di tortura e di pene o trattamenti crudeli, inumani o degradanti: la sentenza Dobbs e gli obblighi di diritto internazionale degli Stati Uniti d'America', (DEP – Deportate, Esuli e Profughe', 2023) <https://www.unive.it/pag/fileadmin/user_upload/dipartimenti/DSLCC/documenti/DEP/finestra/Finestra3_2023.pdf> accessed 26 April 2023.

human rights.⁵ Only at the regional level the Maputo Protocol, the Additional Protocol to the African Charter on Human and People's Rights which concerns the rights of Women in Africa, at art 14(2)(c) mentions medical abortion.⁶ It provides for State Parties to authorize medical abortion 'in cases of sexual assault, rape and incest' while also acknowledging the possibility of undergoing abortion in those cases in which the mental and physical health of the mother might be endangered or, the life of the mother and that of the foetus might be at risk.

Hence, the right to abortion has been anchored to other human rights, such as the right to health. The right to health is inscribed within the International Covenant on Economic, Social and Cultural Rights (ICESCR), at art 12, stating that State Parties are under the obligation to ensure that individuals enjoy the 'highest attainable standards of physical and mental health'.⁷ Although the right to the highest attainable standard of health applies to every individual, Chinkin and Charlesworth have pointed out the gender bias with which human rights have been conceived, extending it to human rights such as those included within the ICESCR and underlying the male centric approach that human rights often include.⁸ As Sifris pointed out starting from the same premises: 'while to most women it seems obvious that reproductive health is an essential component of the right to health, this is not obvious in the context of a system that has traditionally sidelined women's issues'.⁹

The Committee on Economic Social and Cultural Rights (CESCR) clarified in its General Comment No. 14 that the right to health entails freedoms as well as obligations and that those freedoms include the liberty of individuals to control their own health and body, as well as sexual and reproductive freedom.¹⁰

5 See: Erdman (n 4); Sifris (n 4) 186. See also, *Case of Manuela et al v. El Salvador* (Interpretation of the Judgment on Preliminary Objections, Merits, Reparations and Costs) Inter-American Court of Human Rights Series C No 441 (2 November 2021); *Case of Manuela et al v El Salvador* (Partially Dissenting Opinion of Judge Eduardo Vio Grossi) 6.

6 Maputo Protocol art 14(2)(c). See also: De Vido (n 4), p. 46; Charles G. Ngweni, 'Inscribing Abortion as a Human Right: Significance of the Protocol on the Rights of Women in Africa' [2010] 32 Human Rights Quarterly 783, 864.

7 International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 999 UNTS 3 (ICESCR).

8 Christine Chinkin and Hilary Charlesworth, *The boundaries of international law* (Manchester University Press 2022) 231 ff.

9 Sifris (n 4) 193.

10 UN Committee on Economic Social and Cultural Rights, 'General Comment No 14: The Right to the Highest Attainable Standard of Health' (11 August 2000) UN Doc E/C.12/2000/4. Concerning States' obligations in regards to health and removing barriers to health care, it is important to mention that the Convention on the Elimination of all Forms of Discrimination against Women, again at art 12, states the obligations of State Parties in regards to women's health care and underscores that State Parties have to ensure access to health care services including those related to family planning.

The Comment includes core obligations for States to ensure the enjoyment of the right to health and among those of comparable priority includes the need to ensure reproductive, maternal and child health care. When addressing the specific legal obligations, there is no specific mention to abortion, although CESCR stated that:

States should refrain from limiting access to contraceptives and other means of maintaining sexual and reproductive health, from censoring, withholding or intentionally misrepresenting health-related information, including sexual education and information, as well as from preventing people's participation in health-related matters.¹¹

The fact that a clear mention to the right to abortion is lacking should not be interpreted as proof of the fact that the right is not protected under international law, but rather as demonstration of what Chinkin and Charlesworth have argued. Namely, human rights tend to have a male-centric interpretation and approach and for that reason, the way in which reproductive rights have so far been interpreted has resulted in side-lining such issue.

Apart from the already mentioned Maputo Protocol, which openly recognises women's right to reproductive freedom, as well as women's right to abortion, no acknowledgment of women's reproductive rights is found in other international binding documents. A definition of the concept of reproductive rights was offered by the UN Population Division, which stated that:

Reproductive rights embrace certain human rights that are already recognized in national laws, international human rights documents and other relevant United Nations consensus documents. These rights rest on the recognition of the basic right of all couples and individuals to decide freely and responsibly the number, spacing and timing of their children and to have the information and means to do so, and the right to attain the highest attainable standard of sexual and reproductive health. It also includes the right of all to make decisions concerning reproduction free of discrimination, coercion and violence as expressed in human rights documents.¹²

Sifris¹³ has provided a comprehensive list of how reproductive rights branch out, including the right to birth control and to terminate a pregnancy; the right to choose the method of childbirth and to receive proper education and information on the matter, as well as to receive accurate education concerning sex; and lastly, the right to decide the number of children. This latter aspect could be read as both entailing the decision of having a larger family, or a family with

11 *ibid.*

12 United Nations Population Division, 'Report of the International Conference on Population and Development' (5-13 September 1994), UN Doc A/CONF.171/13. See also: Sifris (n 4).

13 *ibid.*

no children. The notion that this paper adopts of ‘family’ is therefore different from the one which has been mostly recognised at the legal level, which centres around reproduction, on the procreation of children. Indeed, Chinkin and Charlesworth have stressed that central to human rights treaties is the notion of family, which is presented as the fundamental group unity of society but the model which is assumed is that of the heterosexual married couple with children.¹⁴ For instance, the recent work of Clarke and Haraway¹⁵ offers a different conceptualization of family, which exceeds the boundaries of traditional families by proposing the concept of ‘making kin’. Families should not be considered such only on the requirements of matrimony (hence of a legal recognition) and on children, either on the way or already present, but they should rather rely on the connection and relationship that human beings (and non-human beings) form with and amongst each other.

Claiming that reproductive rights are still not inscribed in any international legally binding document is not reason enough to state that there is no foundation for the right to abortion at the international level. Moreover, as Sifris pointed out, approaching abortion from the perspective of only one fundamental right, hence developing a one-directional approach leads to oversimplifications of an issue which spans out to several other human rights.¹⁶ The foundations of the right to abortion have been framed within several already existing rights: the right to life, the already mentioned right to health, the right to be free from cruel, inhuman or degrading treatment, the right to be free from discrimination and the right to equality. Restricting, limiting or criminalizing access to abortion amount to violations of such rights under international law. Furthermore, De Vido has conceptualized the criminalization of access to abortion as a form of State’s violence against women and against the reproductive health of women.¹⁷ Particularly, De Vido underlines:

When access is withheld because abortion clinics do not exist in the area where the woman lives, or because practitioners opt for conscientious objection, or

14 Chinkin and Charlesworth (n 8) 232.

15 Adele Clarke and Donna Haraway, ‘Making Kin’: Fare parentele, non popolazioni (Derive Approdi 2022). The authors propose a reconceptualization of the notion of family, starting from feminist considerations linked to climate crisis discourses, which are against the pro-birth rate policies which have been in place up until now. They infer that instead of biological families, we should refer to ‘elective’ families or to ‘logical’ families, hence groups of people which are not related only by blood but by the meaningful connections that they create throughout their lives. Such families are not limited to human beings but can and – according to Haraway – should include non-human animals as well.

16 Sifris (n 4) 189.

17 De Vido (n 5): the author contends that States should be viewed as perpetrators of violence against women and against women’s health. By enacting laws and policies which criminalize abortion, from a vertical dimension, the State is responsible of violations of the positive obligations concerning violence against women’s health under international law.

because the fees are too high, or because the law does not allow women access to abortion and they are obliged to travel, it is evident that these health laws and policies cause violence against women's health (VAWH).¹⁸

International law is still lacking behind in providing full and formal recognition to women's reproductive rights and to the right to abortion. Yet, obligations stemming from international human rights law oblige States to ensure women's reproductive rights and the right to abortion under the framework of other human rights. Indeed, the right to abortion should be granted under the right to health, since abortion is a health issue. Furthermore, restrictions and limitations on abortion have detrimental effects on the health of women – both mental and physical – since they are forced to either travel long distances to undergo abortions legally, or to resort to illegal means which significantly impacts their mental health, adding pressure to an already stressful situation. Moreover, the mental health repercussions of having to carry to term an unwanted child, either because they were the result of a rape or simply because the woman has decided that she does not want to have children should be taken into account, since, in the future, it will not only affect the mother but also the child¹⁹ Human rights apply to individuals, irrespective of sex: the right to health therefore includes, *per se*, sexual and reproductive health as well as the right to abortion.

Moreover, abortion is also a matter of equality, of non-discrimination and autonomy, since it impacts women *because* they are women and should therefore be granted due to the obligations of non-discrimination and the right to equality and autonomy. Criminalizing access to abortion amounts to a violation of *jus cogens* norms, namely from the prohibition of cruel inhuman or degrading treatment. Forcing women to resort to illegal and usually unsafe abortion methods, to experience situations which impact their autonomy, and their dignity amounts to torture or ill treatment. Last but not least, limiting and criminalizing access to abortion is a form of violence against women and women's health as conceived by De Vido, and States should refrain from creating conditions which facilitate VAWH.²⁰

3. Telehealth, telemedicine and telecare

Although the concepts of telehealth, telemedicine and telecare might seem as recent developments in the field of medical care, early applications of

18 *ibid.*

19 Henry P David, 'Born Unwanted: mental health costs and consequences' [2011] 82 *The American Journal of Orthopsychiatry* 184, 192.

20 See: De Vido (n 4), but also Sara De Vido, "'Under His Eye': riflessioni sul ruolo della tecnologia sul corpo delle donne a seguito della sentenza *Dobbs* della Corte Suprema degli Stati Uniti' [2023] *BioLaw Journal* 343, 359.

telemedicine date back to the invention of the ECG by Wilhelm Einthoven at the beginning of 1900,²¹ showing that developments in technology and in medicine have gone hand in hand since the beginning of the 20th century. After that, specialized fields such as radiology and neurosurgery have started to implement technological developments which have become a routine practice, with the use of digital images being a fundamental tool to deliver healthcare for instance.²² At the same time, telemedicine started to become useful in those fields in which there was a need for health care services to be delivered despite the physical distance, such as the case of NASA, where telehealth was used to monitor the health condition of astronauts, or in scientific expeditions in the Antarctic. In this case, for several months weather conditions are particularly adverse and might prove difficult to overcome in case of emergencies. Although medical staff is usually present in expeditions, there might be the need for a specialist who is not among the staff at that time, therefore telemedicine becomes valuable and useful.²³

Since then, telemedicine has further improved and become more and more embedded in people's lives. For instance, in the field of telecare, third generation²⁴ telecare systems are now extremely advanced and have improved up to the point of being referred to as 'lifestyle monitoring': indeed, these devices are able to measure, collect and analyse data in the users' homes. These data can be accessed by the users themselves, relatives or their physicians and provide a clearer picture of the patient's habits. Other devices trigger an alarm when they detect specific hazards without the need for the user to trigger it themselves. This is followed by a call, which can be to a relative or to an appropriate responder up to the level of an ambulance in case the patient is in need. Interestingly, the alarm also sends signals to the patients within their homes which can occur 'through an audible alarm, flashing lights and even vibrating pillows to wake the user from sleep'.²⁵ The use of these devices has increased especially due to the COVID-19 pandemic which, in the case of diabetes management for instance, has helped patients who need to have frequent checks with their physicians in the most chronic cases. The tools implemented in diabetes management are not

21 Sarah Stowe and S Harding, 'Telecare, telehealth and telemedicine' [2011] 1 *European Geriatric Medicine* 196.

22 *ibid.*

23 Adam William Darkins and Margaret Ann Cary, *Telemedicine and Telehealth* (Springer 2000) 8, 9.

24 There is also a first and second generation of telecare devices, see: Stowe and Harding (n 21) 194. See also: Yasser El-Miedany, 'Telehealth and telemedicine: how the digital era is changing standard health care' [2017] *Dove Press Journal: Smart Homecare Technology and Telehealth* 43, 51.

25 *ibid.*

limited to devices, they also include virtual visits, telemonitoring, secure electronic communications either via message or phone calls.²⁶

The use of devices and technology related to medical issues has been referred to in different manners: telecare, telehealth and telemedicine, or even e-health. The World Health Organization (WHO) Guidelines have adopted the following definition of telemedicine:

the provision of healthcare services at a distance with communication conducted between healthcare providers seeking clinical guidance and support from other healthcare providers (provider-to-provider telemedicine); or conducted between remote healthcare users seeking health services and healthcare providers (client-to-provider telemedicine).²⁷

Still, different definitions and interpretations have developed, focusing on different aspects: Darkins and Cary quote at least four different notions of telemedicine, from the simplest ones which define it as 'health care carried out at a distance',²⁸ with the physical element being the only element worth noticing, to others which almost mirror the one provided by the WHO.

All definitions have some common features: they stress the fact that the physical presence is not a necessary element, since being in person face to face with the physician is not instrumental for the health care service to be carried out. This is replaced by the distance communications referred to in the WHO definition, which can happen through phone calls, messaging systems and / or videoconferences. Although Darkins and Cary opt for an all-encompassing approach, stating that it should be based on individual preferences which definition to adopt, they do however understand the need of the WHO to distinguish between telehealth and telemedicine. Telehealth is conceived by the organization as 'the integration of telecommunications systems into the practice of protecting and promoting health',²⁹ while telemedicine concerns the incorporation

26 Rajnish Dhediya, Manoj Chadha, Arpan D. Bhattacharya, Shreerang Godbole and Shreeharsh Godbole, 'Role of Telemedicine in Diabetes Management' [2023] *Journal of Diabetes Science and Technology* 775. See more on telemedicine and its current uses in Ramesh Madhavan and Shahram Khalid, *Telemedicine* (InTech 2013).

27 World Health Organization, 'WHO guideline: recommendations on digital interventions for health system strengthening' (2019) <<https://apps.who.int/iris/handle/10665/311941>> accessed 26 April 2023.

28 Darkins and Cary (n 23) 2, 3. Other definitions provided by Darkins and Cary are: 'Telemedicine involves the use of modern information technology, especially two-way interactive audio/video communications, computers, and telemetry, to deliver health services to remote patients and to facilitate information exchange between primary care physicians and specialists at some distances from each other' and also: 'telemedicine – the use of advanced telecommunications technologies to exchange health information and provide healthcare services across geographic, time, social and cultural barriers'.

29 *ibid.*

of those systems into curative medicine, therefore focusing more on the clinical aspect. According to the WHO, telehealth corresponds to the activities that the organization itself carries out at the international level in the field of public health, since it covers public and community health as well as development of health care systems and epidemiology.³⁰ On the other hand, the definition of telecare is more focused on the aspect of communications, and precisely to the use of technological tools and devices in order to communicate with the patient and deliver health care directly. Stowe and Harding refer to it as a tool to support individuals and professionals in health care delivery.³¹

3.1 Where does Teleabortion situate itself?

The definition of telemedicine which this paper considers as the basis upon which to build its argument is the one provided by the WHO. Teleabortion fits the parameters of the above-mentioned *client-to-provider* telemedicine, since it is usually women who seek the help of physicians and health care professionals to undergo abortions. The WHO Abortion Care Guideline of 2022 speaks of ‘telemedicine approaches to delivering medical abortion care’, refraining from using the term Teleabortion specifically or the alternative *e-abortion*, which refers to the same practice. In recommending that telemedicine, where available, be offered as an alternative to in-person options to access abortion, the Guideline does not provide an exact definition of Teleabortion, but rather operates a distinction, where medical abortion refers to the intaking of drugs (mifepristone and misoprostol) to end a pregnancy as opposed to surgical abortion, which refers to the removal of the foetus through surgical means.³²

Definitions can be found in literature (although still scarce); for instance, Chong *et al* have referred to it as ‘telemedicine abortion’ and defined it as ‘broad term that describes the use of telecommunications (phone, videoconference, texting, email) to provide one or more aspects of abortion care such as counseling, eligibility assessment, medication provision, guidance through the process, and follow-up assessment’.³³ The reason behind the fact that the literature

30 *ibid.*

31 Stowe and Harding (n 21) 193. The authors recall also the definition provided by Barlow *et al*, see: James Barlow, Debbie Singh, Steffen Bayer and Richard Curry, ‘A systematic review of the benefits of home telecare for frail elderly people and those with long-term conditions’ [2007] 13 *Journal of Telemedicine and Telecare* 172, 179.

32 World Health Organization (WHO) and Human Reproduction Programme (HRP), ‘Abortion Care Guideline’ (World Health Organization 2022).

33 Erica Chong *et al*, ‘Expansion of a direct-to-patient telemedicine abortion service in the United States and experience during the COVID-19 pandemic’ [2021] 104 *Contraception* 43, 44. Fang and Perler on the other hand simply state that teleabortion refers to providing medications for abortion via telemedicine, hence a more restrictive definition of the practice. They add that telemedicine refers to use of remote health care services which are delivered through the help of technology, usually a phone or communication via internet. See: Katherine Fang

on Teleabortion is, especially from the international law perspective, still scarce, is that the practice is rather recent and has emerged particularly due to the recent threats to the right to abortion and as a response to the COVID-19 pandemic.³⁴ The pandemic has necessarily determined a change in the way in which abortion services were thought since women could not easily access hospitals to undergo abortions during the pandemic. Moreover, in countries such as the US, the pandemic has also caused a lack in financial means for some women, who were no longer able to pay for the service, due to a loss of income.³⁵ For these reasons, some hospitals in the US, as well as abortion providers more in general, have started to slowly incorporate telemedicine tools and services to provide women with the possibility of terminating their unwanted pregnancies.

Terminating a pregnancy usually entails two phases, divided in abortion care and follow-up or post-abortion care. These two phases characterize Teleabortion as well, although the means through which it is carried out differ from in-person ones. The first phase of Teleabortion relies on the use of telecommunications such as emails, phone calls and messaging systems and/or videoconferences: with the help of these means, women seek the counsel of physicians and abortion service providers. In this phase, women receive counselling and instructions on the next steps, while an eligibility assessment is also conducted: women could be asked to undergo some tests easily accessible at local labs, clinics, or hospitals.³⁶ Once that eligibility has been assessed, the second phase begins, which consists in receiving through mail the *abortion pills*, namely mifepristone and misoprostol. The second phase includes follow-up after drugs-intaking to assess that the pregnancy has been terminated, and in supporting women as to the next steps, such as for instance which contraceptives to use after the abortion.

The WHO Guideline specifies that there is no single recommended approach to delivering abortion services, since it heavily relies on the decisions made by the patient, from the service provider to the location. Yet, it also stresses that while approaches might be different, some conditions must be ensured, namely: access to scientifically accurate and comprehensible information; access to quality assured medicines – particularly relevant in the case of medical or

and Rachel Perler, 'Abortion in the Time of COVID-19: Telemedicine Restrictions and the Undue Burden Test' [2021] *Yale Journal of Law and Feminism* 135, 151.

34 On this note, see: Chong (n 33); Fang and Perler (n 33); see also: Margit Endler, A Lavelanet, A Cleeve, B Ganatra, R Gomperts, K Gemzell-Danielsson, 'Telemedicine for medical abortion, a systematic review' [2019] *BJOG: An International Journal of Obstetrics and Gynecology* 1094, 1102.

35 Chong (n 33) 44.

36 Ibid. See also: Mohana Ravindranath and Darius Tahir, 'Virtual medicine may be the future of abortion' (Politico, 28 October 2020) <<https://www.politico.com/newsletters/future-pulse/2020/10/28/virtual-medicine-may-be-the-future-of-abortion-791238>> accessed 26 April 2023.

Teleabortion; back-up referral support and support in choosing post-abortion contraceptives. The Guideline also stresses that sexual and reproductive health services must be available, accessible, affordable, acceptable and of good quality. Particularly, the ‘delivery of services must be respectful of the culture of individuals, minorities, peoples and communities, and sensitive to gender, age, disability, sexual diversity and life-cycle requirements’.³⁷

4. Teleabortion from the perspective of women’s rights

4.1. The advantages of Teleabortion

Abortion is first and foremost a women’s issue, and limitations or restrictions aimed at impairing access to the service affect women because they are women. Another aspect should be considered, once the gender dimension of abortion has been laid out, namely the intersectional lens: abortion affects women in a different way. An intersectional approach³⁸ to abortion is necessary to identify and highlight how women from different backgrounds experience and are affected by abortion in different ways. This discussion could be widened to encompass women’s reproductive rights more in general, starting from methods of contraception³⁹ for instance, but due to space constraints the discussion will be focused on abortion. Indeed, women and young girls coming from ethnic minorities and marginalized groups are more deeply affected by limitations of access to abortion.

The overruling of *Roe v Wade*,⁴⁰ the US Supreme Court judgement which granted women the right to abortion in the US, has indeed demonstrated how restrictions on access to abortion affect women differently. In *Dobbs* the Supreme Court restored a power which should have been prerogative of the legislators in the first place – according to the majority of the judges: each State can now decide whether to restrict, limit or criminalize abortion. This means that not only women seeking and undergoing abortions in those States might be arrested, but also those helping women undergoing abortions, such as professionals and healthcare facilities would commit criminal acts under the newly passed legislations. Thirteen States have already banned abortion throughout the pregnancy, authorizing it only in specific cases in which women might face serious or certain health consequences: for instance, Utah allows abortion in

³⁷ WHO and HRP (n 32).

³⁸ Kimberlé Crenshaw, ‘Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics’, [1989] 1 The University of Chicago Legal Forum 139, 167.

³⁹ Clarke and Haraway (n 15) 34.

⁴⁰ *Jane Roe, et al v Henry Wade* [1973] USSC 70-18, 410 US 113.

case of foetus abnormalities, and Louisiana allows exceptions to the abortion ban in case in which the pregnancy is deemed as 'medically futile'.⁴¹

At the same time, States such as California, Delaware and Connecticut have expanded the eligibility criteria for reproductive care services,⁴² aimed at including also those women who live in those States which have enacted abortion bans. Still, not all women can afford to travel to a different or even neighbouring country if in need of terminating a pregnancy, and this affects especially women from marginalized groups, ethnic minorities, but also young girls who either do not have the means to travel nor information on how to access reproductive care services. In this context, Teleabortion would provide particularly instrumental and useful: internet connection is available almost everywhere in the US and devices to access it can be easily found. Smartphones and devices which connect to the internet, tablets and personal computers are part of many people's lives, especially after the COVID-19 pandemic, which has underscored the necessity of having access to the internet. Teleabortion would be an alternative in those Countries where access to the internet can be easily achieved, not a worldwide solution to the issue of restrictions on abortion.

The case of young girls is particularly relevant to demonstrate the advantages of Teleabortion. The Special Rapporteur on the right to health highlighted in the 2016 Report that '[a]dolescents face multiple barriers to health services, including the following: restrictive laws and policies; unavailability of contraception or safe abortions' and that 'lack of awareness or understanding of their unique health needs can render adolescents invisible'. Moreover, the report stressed that: '[a]dolescent sexual and reproductive health services must be welcoming, adolescent-friendly, non-judgmental and guarantee privacy and confidentiality'.⁴³ The argument that Teleabortion is particularly adolescent-friendly could be advanced especially if one were to look at the tools it relies upon: most young girls who have access to a smartphone, a tablet, or a computer and to an internet connection could potentially access Teleabortion services.⁴⁴

In terms of its advantages, it should be noted that the WHO conducted a systematic review, which features in the Abortion Care Guideline of 2022, on the use of telemedicine and medical abortion. The report confirms the safety of medical abortions and that no significant differences were noticed as

41 Nicole Dube, James Orlando and Jessica Schaeffer-Helmecki, *Research Report on State Abortion Laws Enacted Post-Dobbs Decision* (Office of Legislative Research, 2022-R-0227, 2022) 1, 20.

42 *ibid.*

43 Human Rights Council, 'Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health' (4 April 2016) UN Doc A/HRC/32/32.

44 According to ITU (International Telecommunication Union) 80% of people between the ages of 15 and 24 can access the internet. See: <<https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-youth-internet-use/#:~:text=Almost%2080%20per%20cent%20of,and%2024%20use%20the%20Internet>> accessed 7 January 2025.

opposed to in person medical abortion care services. Controlled trials and observational studies have been conducted in Bangladesh, Cambodia, Egypt and Indonesia, Canada, Peru and the USA. According to the Guideline: ‘there was no difference between the two groups in rates of successful abortion or ongoing pregnancies. Referrals for surgical intervention were fewer among women who used telemedicine. Satisfaction with telemedicine services was high and comparable to the usual clinical services’.⁴⁵ Therefore, resorting to telemedicine and medical abortion is safe and as effective as surgical abortions and should be allowed where available.

Beside safety and efficacy, the advantages provided by Teleabortion are first and foremost the potential outreach of the service. Clinics which grant access to the service, have the possibility of reaching a wider range of women who would not be forced to travel physically to a clinic or hospital, or, in cases where abortion bans are in place, to another country since they would be able to interact with a professional through a video conference. Consequently, Teleabortion entails also a significant reduction in costs, since travel expenses are ruled out and also the cost of the service is substantially reduced, hence, allowing a broader number of women and young girls to access it. In the wake of the overruling of *Roe v Wade*, women from one of the states which have enacted bans on abortion would have to travel abroad to get one. This would entail having the means to afford such travel, since they would have to bear all the costs of the procedure, and – De Vido warns – also those of risks due to possible medical complications.⁴⁶

Another fundamental aspect that speaks in favour of Teleabortion is the opportunity of avoiding a common phenomenon which women undergoing abortion experience also in those countries in which the right is granted, which this paper refers to as abortion-related obstetric violence.⁴⁷ This term indicates the humiliating comments and practices, names-calling and psychological abuse which women seeking abortion tend to experience in hospitals, perpetrated by those among the medical staff who oppose abortion. Examples of such abuses

45 WHO and HRP (n 32).

46 De Vido (n 4) 144.

47 This phenomenon has been referred in this way by some scholars or as obstetric violence related to abortion. It has been mostly discussed in those Countries in which abortions are performed by the obstetric staff. In Italy, for instance, such practice would still be unnamed, due to the fact that the medical staff involved in abortion procedures is not the obstetric one, even though there are substantial numbers of accounts of women seeking abortion in Italy who have experienced such abuse. See: Juliana Tamayo Muñoz et al. ‘Obstetric Violence and Abortion. Contributions to the Debate from Colombia’ (Grupo Médico por el Derecho a Decidir, November 2015) <https://globaldoctorsforchoice.org/wp-content/uploads/Obstetric-Violence_and_Abortion_EN-final-1.pdf> accessed 26 April 2023; Lorenzo Bernardini, Sara Dal Monico, ‘A Way Forward: Criminal Law as a Possible Remedy in Addressing Gynaecological and Obstetric Violence?’ [2024] 95 2 International Review of Penal Law 269.

are recalled by women worldwide, and the psychological impact that such violence has on women has been recognised as amounting to torture or ill treatment, by the UN Special Rapporteur on torture and other forms of cruel, inhuman or degrading treatment.⁴⁸ De Vido has well underlined that such violence is enacted also through laws and policies, and one of the most significant in the context of abortion is ultrasound: women are obliged to listen to the sound of the foetus' heartbeat or to look at the screen and see its image, even if the need for such practice is not supported by scientific evidence.⁴⁹

Teleabortion is safe and appears as cost effective while also offering the opportunity for a wider range of women and young girls to access the service, which would help avoiding that abortion becomes available only to a restricted number of women. Furthermore, due to the fact that it relies on internet connection, videoconferences and messaging (either via email or texts) it is widely available (not everywhere of course, but this matter will be addressed in the following paragraph). Last but not least, it would allow women to access the service from a – possibly comfortable – location of their choice and avoid the psychological and emotional toll of going to the hospital, which can be per se a traumatic experience for women, not to mention instances in which they are

48 Human Rights Council, 'Report of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment' (5 January 2016) UN Doc A/HRC/31/57.

49 The need for performing an ultrasound is not questioned here, but the practice of showing the image to women or force them to listen to the heartbeat is. Women undergoing ultrasounds should not be forced by law to look at the image or listen to its heartbeat but could be asked if they want to. If the aim of such practices is to give women full knowledge of what is happening, then they should be able to decide whether or not they want to look at it or listen to it. Forcing this upon them could constitute a form of violence against women's health, a violation of their reproductive rights and of their right to autonomy. See further: De Vido (n 4) 160. On the scientific relevance of performing ultrasounds in case of abortion, see: Jen Russo, 'Mandated Ultrasound Prior to Abortion' (AMA Journal of Ethics, 2016) <<https://journalofethics.ama-assn.org/article/mandated-ultrasound-prior-abortion/2014-04>> accessed 26 April 2023; Marianne Kielsvik, Ragnhild JT Sekse, Elin M Aasen, and Eva Gjengedal, 'Viewing the image? Ultrasound examination during abortion preparations, ethical challenges' [2022] 29 Nursing Ethics 511. The authors have conducted a study in Norway where women wishing to undergo abortion were asked whether they wanted to see the image of the foetus or listen to the heartbeat, since the country does not require that by law, while ultrasound are common practice. It is also reported that while in Norway no law mandates such practice, and in the UK it is recommended that women are given the option, in the USA some States require by law that women are shown the image and, when present, forced to listen to the heartbeat, thus showing that no scientific evidence supports such choice, which is, in fact, a choice. Lastly, see: Sophie Wylomanski and Norbert Winer, 'Role of ultrasound in elective abortions' [2016] 45 Journal de Gynécologie Obstétrique et Biologie de la Reproduction 1477, 1489. The authors underline how in the case of women who are positive about the dates of their last cycle and/or of the sexual encounter at risk, ultrasound should not be forced or even, its lack should not impair their ability to access abortion.

later shamed and degraded by hospital staff.⁵⁰ Furthermore, as most telemedicine tools, it can be considered as user-friendly: women are followed step by step by physicians and/or service providers and once they have received the drugs at the designated location, they should have been carefully instructed on how to proceed.

4.2 Where it gets tricky: Teleabortion and women's right to privacy

Teleabortion is not a world-wide applicable solution to allow access to abortion. The opportunity offered by this technology is in some way limited to those countries where access to a device with internet connection is easily available, which therefore would not be the case for most developing countries. Moreover, access to internet does not always equal knowing how to use or navigate it, which could possibly restrict the range of women even more. The International Telecommunication Union (ITU), the UN specialized agency for information and communication technologies has assessed that 2.9 billion people worldwide are still offline, which adds up to almost 37% of the world population. Although a growth in internet users has been noticed, there is still a large portion which does not have access to it making access to the internet unbalanced.⁵¹ This would entail, in the context of Teleabortion, that due to the lack of availability of the main element and, consequently, a lack in telemedicine services altogether, it cannot be regarded as a worldwide applicable option for women wishing to end their pregnancies. Teleabortion limits to those areas of the world where telemedicine has developed and where connection to internet is granted and easily accessible. It should also be noted that ITU highlighted a gender gap in internet access: as of 2021, 62% of internet users are men compared to 57% for women.⁵²

The second biggest concern in the context of Teleabortion and one of the crucial aspects investigated by this paper relates to the issue of privacy and data

50 On this note, see: Sara Larrea, Mariana Prandini Assis and Camila Ochoa Mendoza, "“Hospitals have some procedures that seem dehumanising to me”: Experiences of abortion-related obstetric violence in Brazil, Chile and Ecuador" [2021] 35 *Agenda* 54, 68.

51 See ITU, 'Facts and Figures 2021: 2.9 billion people still offline' (2021) <<https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline/>> accessed 26 April 2023. On the right to access internet, which has been discussed at the UN level, see: Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) UN Doc A/HRC/17/27, which does not speak of a human right to access internet per se but refers to accessing the world wide web as an 'enabler' for other human rights. See also: Oreste Pollicino, 'The Right to Internet Access: Quid Iuris?' in Andreas von Arnould, Kerstin von der Decken and Mart Susi (eds), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (CUP 2020) 263, 275.

52 ITU, 'Global Connectivity Report 2022' (2022) <<https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/>> accessed 26 April 2023.

protection. The right to privacy is protected at the international level under the ICCPR and particularly at art 17. This article provides the right of every person to be protected against unlawful interferences in their private sphere, family life or home which might be enacted by State authorities but also from legal and natural persons. State parties are under an obligation to adopt legislative measures to prohibit such interferences.⁵³ The Special Rapporteur on the right to privacy has also highlighted that it is not an absolute right but a qualified right, which can be limited but in a 'carefully delimited way'.⁵⁴ In its 2021 report, the UN High Commissioner for Human Rights stated that the right to privacy is a cornerstone for a democratic society. Moreover, the report stated that the right to privacy 'is an expression of human dignity and is linked to the protection of human autonomy and personal identity'.⁵⁵ Although the report, which focuses on the right to privacy in the digital age, does not provide a comprehensive understanding of how privacy and human autonomy intertwines with sexual and reproductive autonomy, the link has been reiterated by human rights courts at the regional levels. For instance, the Inter-American Commission of Human Rights (IACommHR) has stressed in the case *López Soto et al v Venezuela* that the violence which Linda López Soto suffered amounted to a violation of her right to privacy, autonomy and dignity. In this case, Linda was kidnapped and sexually assaulted (therefore, it is not strictly linked to the abortion issue) but both the report and later the judgement by the court (IACtHR) reiterated that violations of her sexual and reproductive autonomy would hinder her right to privacy as well, which in this context refers to the aspect of privacy attaining to right to private life.⁵⁶

53 UN Committee on Civil and Political Rights, 'General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc. HRI/GEN/1/Rev.1.

54 Human Rights Council, Fortieth session, 25 February–22 March 2019, 'Report of the Special Rapporteur on the right to privacy' (16 October 2019) UN Doc. A/HRC/40/63. The right to privacy can be limited provided that such interferences be neither arbitrary nor unlawful. It was the Human Rights Committee that clarified in their General Comment No. 16 that 'unlawful' refers to interferences which are not envisaged by law, which are therefore prohibited, and that 'arbitrary' interferences refers also to those which can be envisaged by law but that act in contrast with the object and purpose of the Convention. These two guarantees have been introduced to safeguard the right to privacy and the requirement of arbitrariness is particularly relevant in this context since it aims at safeguarding the private life of individuals from interferences which may be introduced by law, hence lawful, but that infringe on the rights provided under the Convention. See *ibid.*

55 Human Rights Council (n 3).

56 *Case of López Soto et al v Venezuela* (Interpretation of the Judgment on Merits, Reparations and Costs) Inter-American Court of Human Rights Series C No. 379 (14 May 2019). See also De Vido (n 4) 148. De Vido also recalls another report from the IACommHR, concerning the case *Manuela y Familia v El Salvador*, in which a woman was detained after having a miscarriage and later died while being imprisoned. Within its report, the IACommHR mentioned the connection between freedom from violence and the rights to personal integrity, 148. This

At the European level, the European Court of Human Rights (ECtHR) has adopted a careful approach in addressing the right to abortion, which according to its jurisprudence is protected under art 8 of the European Convention on Human Rights (ECHR). This article protects the right to respect for private and family life, home and correspondence and the court has used it, by broadly interpreting the notion of private and family life, in cases of abortion. Yet, as Fenwick notices:

At first glance, it might appear anomalous that the Convention jurisprudence on Article 8, which has adopted an expansive concept of “private life”, encompassing broad rights associated with personhood and the environment, has not decisively recognised that women have a right to choose to terminate their pregnancies. In the modern abortion jurisprudence, the Court has firmly refused to allow its stance to be freighted with the typical values underpinning Article 8 as to bodily autonomy.⁵⁷

The breadth of the right to privacy is much wider than reproductive rights, clearly. Although connected and deeply intertwined with the right to abortion,⁵⁸ the right to privacy covers and widens to other aspects. In the context of Teleabortion, one aspect of the right to privacy is particularly relevant apart from the already mentioned connection with women’s reproductive rights: the

case is also particularly relevant because the victim was also actively prevented from accessing abortion, which is not allowed in El Salvador. The IACtHR, in its judgement of 2021, found El Salvador responsible for the violation of Manuela’s right to free from cruel, inhuman or degrading punishment under the American Convention on Human Rights, due to her detainment and the mistreatment at the hospital, which includes the denial of undergoing abortion.

57 Fenwick (n 4) 273. The author also underlines how different the approach of the ECtHR is from that of the Supreme Court of the USA undertaken in *Roe v Wade*, where the Supreme Court found that the basis for abortion rights were incorporated within the right to privacy, especially in *ABC v Ireland*. The approach of the ECtHR hence shows a careful and not clear-cut position in favour of women’s right to abortion. See further: De Vido (n 4) 161. Furthermore, in the Guide on Article 8 drafted by the Court, the ECtHR stated that in terms of reproductive rights, when prohibitions to abortion are set in place for reasons of health and/or wellbeing they fall within the scope of art 8 (2), which regulates State’s interferences with the right to private life. See Registry of ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Report, 31 August 2022) 1, 172.

58 Sifris notes that Justice Ruth Bader Ginsburg and Reva Siegel have highlighted the close connection between autonomy and equality in the context of abortion. Indeed, prohibitions aimed at restricting access to abortion violate both the right to autonomy and the principle of equality, hence criticizing the approach taken by *Roe* which altogether trumped the perspective of equality. She continues: ‘According to Siegel, one of the hallmarks of patriarchy is the restriction of women’s autonomy thus there is a clear connection between violations of women’s autonomy and discrimination against women. Similarly, Rebecca J Cook has observed that [t]he pursuit of women’s autonomy requires their reproductive self-determination. Respect for human rights to reproductive self-determination requires the prohibition of all forms of discrimination against women’, Sifris (n 4) 108.

protection of personal data. One of the advantages of Teleabortion is the reduction of costs as well as its availability, which is due to the fact that it relies upon the use of internet connection, email exchanges and videoconferences, etc. To understand more clearly, let us paint the example of a young woman, who is seeking to terminate her unwanted pregnancy through Teleabortion. The first step is to surf the internet and look for providers of that service. The next step is to contact the provider via email or phone call and set up a video conference. Before receiving the drug at home, she will have to undergo – let us say, for the sake of this example – at the bare minimum at least a blood sample exam. She will then send the results, probably via email, or they will be sent to the physician or the provider, who will store them in her file. Let us say that that young woman lives in the USA after the overruling of *Roe v Wade* (although, we could imagine a young woman living in Europe, maybe in Hungary⁵⁹ or in Poland⁶⁰). Let us continue our example, by imagining that the country where she lives is one of those which has enacted abortion ban policies and that she travelled to a relative's or a friend's house, in a nearby country, where the service of Teleabortion is legally provided. She undergoes the procedure, thus terminating her pregnancy and goes back home, the only trace of her unwanted pregnancy being the data exchanged via email and the clinical file stored by the Teleabortion provider.

In the wake of the overruling of *Roe v Wade*, the press in the USA started to share articles and posts which voiced concerns over the possible dangers of AI, due to the fact that some governments had advanced the proposal of creating tip-off lines, where individuals would call and tip-off a neighbour, a friend, a colleague and a patient and receive a bounty for their service.⁶¹ In this case,

59 For instance, on the impact of the Dobbs judgment in Hungary see: Katalin Kelemen, 'Una breve nota sull'impatto della sentenza Dobbs in Ungheria' [2023] *BioLaw Journal* 483, 488. The author suggests that changes in Hungary's legislation only two months after the Dobbs judgment, although different in content, highlight a change in perspective. The 'heartbeat rule' as it is being referred to could be a forerunner of more conservative changes in the national legislation of the country.

60 On Poland, see: Marta Tomasi, 'Abortion Rights e spazio costituzionale europeo: gli orizzonti ristretti dell'ordinamento polacco', [2023] *BioLaw Journal* 403, 415.

61 See: Jeremy Kahn, 'After Roe, fears mount about A.I.'s ability to identify those seeking abortions' (*The Fortune*, 28 June 2022) <<https://fortune.com/2022/06/28/after-roe-v-wade-fear-of-a-i-surveillance-abortion/>> accessed 26 April 2023; Emma Bowman, 'As states ban abortion, the Texas bounty law offers a way to survive legal challenges' *NPR* (11 July 2022) <<https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law>> accessed 26 April 2023. Within her post, the author addresses Texas Heartbeat Law, or Senate Bill No 8 (available here: <<https://legiscan.com/TX/text/SB8/2021>>) which not only bans abortion but also sets up a bounty mechanism for tipping off either women who have undergone or are seeking to undergo abortions as well as those aiding and abetting abortion seekers, namely physicians, abortion providers, drivers or peoples who have helped financially the woman in order to have enough money to undergo the procedure.

which could be a reality in Texas, data coming from apps which track menstrual cycles, walking apps which pinpoint your location, might be used against women where abortion is criminalized. It needs to be stressed that this is still an extreme example, yet it offers insights on how necessary the protection of data concerning health is. From this perspective, international law is still lacking behind. The protection of personal data in regards to health has been underlined at the regional level by the jurisprudence of both IACtHR and the ECtHR. In *Manuela et al v El Salvador* the Court stated:

Even though personal health data is not explicitly established in Article 11 of the Convention, this is information that described the most sensitive or delicate aspects of an individual, so that it should be understood as protected by the right to privacy. Information on an individual's sex life should also be considered as personal and highly sensitive.⁶²

WHO guidelines underline how abortion is a stigmatised and personal matter, hence the worry that confidential data might be disclosed, which in the case of a woman wanting to terminate her pregnancy might be a reason stopping her from using the service, if she fears that such sensitive information is not safeguarded.⁶³ A similar conclusion can be found within the Guide on Article 8 drafted by the Registry of the ECtHR, which in referring to the case *M.S. v Sweden* states that:

The disclosure – without a patient's consent – of medical records, including information relating to an abortion, by a clinic to the Social Insurance Office, and therefore to a wider circle of public servants, constituted an interference with the patient's right to respect for private life.⁶⁴

In the aforementioned report on the right to privacy in the digital age, the High Commissioner for Human Rights has stressed that where there is a high risk for human rights the legal requirements governing the use of AI should be stricter and that sectors such as health where 'the stakes for individuals are particularly high' should have priority. The report also stresses that 'uses of AI

On the possible use of technology in this field as an instrument to control women see also De Vido (n 20) 355. De Vido recalls that a recent report by the Congressional Research Service of the USA has highlighted that federal law in relation to data privacy offers relatively limited constraints to the ability of law enforcement to acquire and use personal data relating to criminal activity. In response, De Vido also recalls actions at the legislative level to prevent local authorities and privates to acquire, use and share data concerning the reproductive health of a person without their written consent.

62 *Manuela et al v El Salvador* (n 5).

63 WHO, 'Guideline Recommendations on Digital Interventions for Health System Strengthening' (World Health Organization 2019).

64 *Guide on Article 8* (n 57) 58.

that inherently conflict with the prohibition of discrimination should not be allowed'.⁶⁵ On a similar note, the report of 2019 by Task Force on Privacy and Protection of Health-Related Data (instituted under the mandate of the Special Rapporteur on the Right to Privacy) was issued with the purpose of providing guidelines on the processing of health-data, emphasizing the need for a legitimate basis. It proposes principles with which data processing should comply such as transparency and fairness of the collection process and that data must be collected for explicit, specific and legitimate purposes 'in a manner which is compatible with the purposes for which it was originally collected'.⁶⁶

In regards to Teleabortion, it can be argued that health data regarding abortion concern women, due to the fact that abortion is a woman's issue. Attempts at criminalizing abortion affect women because they are such, as well as using data for that purpose. It follows that any attempts at using against women health data regarding abortion, and especially those which are instrumental in Teleabortion practices, would constitute a violation of their right to privacy, of the right to non-discrimination and that of equality, since they would be targeted because they are women undergoing a medical procedure which only affects women. The Special Rapporteur highlighted in their report on the gender perspective relating to the right to privacy that while State surveillance is generally portrayed as targeting male individuals, on the other hand 'women can expect that nearly every detail of their intimate lives will be subject to multiple forms of surveillance by State as well as private actors, from domestic violence to sexual objectification and reproduction'.⁶⁷

5. Conclusion

The purpose of this contribution was to investigate the practice of Teleabortion from an international law perspective, in light of the recent attempts to hinder the right to abortion in several countries. In particular, Teleabortion has been considered as a means to women's enjoyment of their reproductive rights: a right to Teleabortion is not being discussed here, as it would fall under the broader category of the right to abortion. Although international law is lacking in terms of an express recognition of the right to abortion, this does not entail that there is no obligation for States to ensure access to the service. Such obligations stem from human rights law and *jus cogens* norms: the criminalization of abortion amounts to cruel inhuman or degrading treatment as it was already underlined, and the right to abortion is inscribed within the

65 OHCHR (n 53) 45.

66 Committee of Ministers of the Council of Europe, 'Recommendation CM/Rec(2019)2 of the Committee of Ministers to the Member States on the protection and use of health-related data' (27 March 2019) CM/Rec(2019)2 [4].

67 Human Rights Council (n 4).

parameters of the right to health and the right to privacy. Criminalizing women seeking abortion affects their rights to equality and non-discrimination as well, since it is a practice which only women can undergo. Moreover, following De Vido's conceptualization of violence against women's health, criminalizing abortion is also a form of violence against women and women's health.

From these premises, the paper has built on how Teleabortion works, highlighting its advantages especially if an intersectional approach is taken into account: it would provide access to the service to a wider range of women since the costs would be significantly reduced, as well as being easily accessible and available. On the other hand, with Teleabortion comes the issue of data protection, which needs to be ensured since health data are particularly sensitive. Lacks in international law in this regard should be addressed: there is no international framework for data protection which entails a lack of harmonization in how data are protected worldwide. An international framework safeguarding health related data seems difficult to imagine. Regional systems have been set in place, with the European Union being at the forefront in terms of data protection.⁶⁸

As a possible solution in terms of the harmonization of data protection practices, Kuner suggests the adoption by non-CoE Members as well of the Council of Europe Convention 108, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data⁶⁹ which after the Amendment of 2018 which saw also the adoption of an additional protocol and is now referred to as Convention 108+, the modernised version. The Convention is open for accession to non-Member States of the Council of Europe, hence presenting a possible universal framework providing the basis for global data protection standards.⁷⁰ Kuner yet warns on the difficulty of finding a possible agreement on global data protection standards and suggests also that some countries might opt for a non-binding set of standards.⁷¹ The Convention deals with health and sexual life data at Article 6, referring to the special categories of data, and states that the processing of these data is only to be allowed where appropriate safeguards have been implemented in national legislations, complementing those of the Convention. Paragraph 2 provides a

68 Christopher Kuner, 'An international legal framework for data protection: Issues and prospects' [2009] 25 Computer Law & Security Review 307, 313; De Vido (n 20) 358, 359: the author came to the same conclusion that so far, the most efficient responses can be found at the regional level, especially at the EU and CoE levels: 'Alla luce del quadro normativo qui descritto, sia nel quadro del Consiglio d'Europa, sia nel quadro del sistema dell'Unione europea, ci sembra difficilmente argomentabile che una restrizione al diritto alla privacy delle donne, mediante geolocalizzazione dei loro spostamenti o mediante comunicazione alle autorità del loro accesso ad un ospedale che pratica l'interruzione di gravidanza, possa giustificarsi alla luce del sistema europeo di tutela dei diritti umani fondamentali' [359].

69 *ibid.*

70 Kuner (n 68) 313.

71 *ibid* [316].

further clarification of safeguards, stating that they 'shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination'.⁷²

Still, Teleabortion is not yet a wide-spread practice and its uses have been mostly concentrated in the USA and South America. However, it is not difficult to imagine its implementation also in Europe since the means and the drugs it relies upon are available as well.⁷³ Indeed, access to the internet is granted almost everywhere in Europe and the drugs necessary to perform medical abortions, namely misoprostol and mifepristone, are used in Europe as well. On a wider scale and for different fields Telemedicine is being implemented in Europe and that might soon include Teleabortion too.

The analysis on Teleabortion has allowed to further reflect on fundamental human rights and it should be clear that Teleabortion touches upon several other rights: the right to abortion, the right to health and the right to privacy. If made available, it is a means to ensure women's reproductive rights. Furthermore, the strength of Teleabortion resides in allowing women to avoid having to deal with the stigma and degradation that oftentimes they face in hospitals, as if the psychological and physical toll of undergoing a pregnancy termination was not difficult enough.⁷⁴ This would be due to the fact that women using Teleabortion services would be followed by physicians who would clearly have to be non-objectors, since, in the USA for instance, the service is provided by pro-choice associations and clinics. Indeed, one of the main barriers that women have to face even where abortion is legal and granted is conscientious objection.⁷⁵ Referral mechanisms⁷⁶ have been discussed at the international level as a possible solution, or another option would be a system of quotas, where States guarantee a certain number of pro-choice physicians, hence willing to perform abortions. Provided that there are not yet positive obligations for States with regard to access to abortion,⁷⁷ there are obligations in this regard stemming from the rights to health, to privacy and autonomy, to non-discrimination and equality.

72 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [2018] CETS. No. 108+.

73 In the case of Italy for instance the NGO Women on Web has been helping women access safe abortion through Teleabortion, allowing women to get a consult online and have the abortion pills sent home. See: <<https://www.womenonweb.org/it/page/521/women-on-web>> last accessed 30 December 2024.

74 On the social stigma attached to abortion see: Sifris (n 4) 212.

75 See: Zoe L Tongue, 'On conscientious objection to abortion: Questioning mandatory referral as compromise in the international human rights framework' [2022] 22 *Medical Law International* 277, 371. See also De Vido (n 4) 55.

76 See: *ibid.*

77 De Vido (n 4) 55.

The EU Digital Services Act: An Assessment in Light of the Rights of Persons with Disabilities

*Anna Facchinetti **

University of Pavia, Italy

ORCID 0009-0009-9777-4742

DOI: 10.54103/milanoup.215.c461

Abstract

The paper tackles the topic of accessibility of services and information for persons with disabilities in the digital domain, with focus on EU law. Its purpose is to assess whether Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) complies effectively with the accessibility obligations set forth in the UN Convention on the Rights of Persons with Disabilities (CRPD), to which the European Union is a party since 2011. It is argued that the Digital Services Act – whose objective is, *inter alia*, to improve consumers' protection and the transparency of platforms – fails to fully protect the rights of persons with disabilities insofar as it makes web accessibility the object of voluntary codes of conduct, rather than of obligations. The paper adopts the doctrinal legal methodology.

Keywords

UN Convention on the Rights of Persons with Disabilities; Web Accessibility; Digital Inclusion; Digital Services Act; Codes of Conduct

1. Introduction

Information and communication technologies (ICTs) – including social media, meant as ‘websites and applications that enable users to create and share

* This research was conducted under the research project “RISID – *Realizing the right to Social Inclusion for persons with Disabilities through new tools of smart communication and sharing knowledge: from international to local effectiveness*”, funded by Fondazione Cariplo.

content or to participate in social networking¹ – can be an instrument of social inclusion for persons with disabilities, but they can also be a source of further exclusion if they are not fully accessible. As set forth in the United Nations Convention on the Rights of Persons with Disabilities (CRPD),² accessibility is necessary for persons with disabilities to enjoy their human rights. Accessibility of services and information, including in the digital domain, is the precondition for the full enjoyment of human rights, independent living and social inclusion of persons with disabilities,³ and a human right *per se*.⁴ The proposed contribution will critically evaluate a recent piece of EU secondary legislation on digital services, namely the Digital Services Act (DSA),⁵ in light of the accessibility obligations set forth in the CRPD, to which the European Union is a party since 2011. To this purpose, the paper will first flesh out the content of the accessibility obligations under the CRPD with specific reference to websites and mobile applications. It will then provide a short overview on the status of the CRPD within the EU legal framework and on other EU binding instruments in the field of web accessibility. It is argued that the Digital Services Act – whose objective is, *inter alia*, to improve consumers’ protection and the transparency of platforms – fails to fully protect the rights of persons with disabilities insofar as it makes web accessibility the object of voluntary codes of conduct, rather than of obligations. The paper adopts the doctrinal legal methodology.

2. Obligations stemming from the CRPD in matters of accessibility

The CRPD, adopted by the United Nations General Assembly in 2006 and widely ratified, evidences the general acceptance at the international level of the

1 Silvia Favalli, ‘Disability, Social Media and Human Rights: “What’s the catch?”’ in Maria Caterina Baruffi and Matteo Ortino (eds), *Trending topics in international and EU law: legal and economic perspectives* (Edizioni Scientifiche Italiane 2019) 19.

2 Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, opened for signature 30 March 2007, entered into force 3 May 2008) 2515 UNTS 3.

3 CRPD Committee, ‘General comment No. 2 (2014). Article 9: Accessibility’, (22 May 2014) CRPD/C/GC/2, para 1.

4 According to the CRPD Committee, albeit a disability-specific concept, accessibility can be traced back to a general right of access to goods and services enshrined in other human rights treaties, such as the Convention against all forms of Racial Discrimination (ibid, para 4). Nonetheless, the literature highlights that accessibility goes well beyond the so-called ‘right to access’ because it entails positive measures and imposes indirect obligations falling upon private parties, and thus amounts to a new human right (Andrea Broderick, ‘Of rights and obligations: the birth of accessibility’, [2020] *The International Journal of Human Rights* 393).

5 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

social model of disability, as opposed to the medical model.⁶ While the medical (and traditional) model of disability focuses on the impairment, regarded as an individual, negative situation which deserves charitable interventions, the social model considers disability as a social construction, resulting from the physical and social barriers that may hinder the full and effective participation in society of persons with disabilities.⁷ The CRPD enhances the social model by codifying a human rights model of disability, which takes into account both the individual impairment and the social construction of disability.⁸ This approach is reflected in the open-ended description of ‘persons with disabilities’ enshrined in the Convention.⁹ Based on art 1(2) CRPD, ‘persons with disabilities include those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others’. Hence the CRPD’s focus on accessibility – also implying the removal of barriers – so as to ensure that persons with disabilities have access, on an equal basis with others, ‘to the physical environment, to transportation, to information and communications, *including information and communications technologies and systems*, and to other facilities and services open or provided to the public, both in urban and in rural areas’.¹⁰

The CRPD addresses ICT accessibility at art 9, on the principle of accessibility, and at art 21, on freedom of expression. Art 9 obliges States Parties to take all the appropriate measures to ensure that persons with disabilities have access to digital information and communication systems, including electronic services. In particular, the Convention includes States’ obligation ‘to promote access for persons with disabilities to new information and communications technologies and systems, including the Internet’ (art 9(2)(g)). Importantly for our purposes, based on art 9(2)(b) CRPD, States must ensure that private entities that offer services open or provided to the public take into account all aspects of accessibility for persons with disabilities, including in the digital domain. The United Nations Committee on the Rights of Persons with Disabilities (CRPD Committee), in its General Comment No. 2 on accessibility, confirmed that private parties are bound by accessibility obligations, if they provide public

6 Emily Kakoullis and Yoshikazu Ikehara, ‘Article 1: Purpose’ in Ilias Bantekas, Michael Ashley Stein, Dimitris Anastasiou (eds), *The UN Convention on the Rights of Persons with Disabilities. A Commentary* (OUP 2018), 54.

7 Silvia Favalli, *Disabilità, diritti umani e diritto internazionale* (Giuffrè 2021), 7-10.

8 *ibid.*, 11-12; Valentina Della Fina, ‘Article 1 [Purpose]’ in Valentina Della Fina, Rachele Cera and Giuseppe Palmisano (eds), *The United Nations Convention on the Rights of Persons with Disabilities. A Commentary* (Springer 2017), 98.

9 In fact, the CRPD does not include a definition of ‘disability’ (defined as an evolving concept in the Preamble, para 13). On the negotiation process, which finally excluded a definition, see: Emily Kakoullis and Yoshikazu Ikehara (n 6), 44-48.

10 United Nations Convention on the Rights of Persons with Disabilities, Article 9(1). Emphasis added.

services.¹¹ Likewise, art 21 CRPD, protecting freedom of expression – including also its passive side, that is ‘the right to seek and receive information so that ideas and opinions can be developed’¹² – binds States not only to provide information to the public in accessible formats (art 21(a)), but also to urge ‘private entities that provide services to the general public, including through the Internet, to provide information and services in accessible and usable formats for persons with disabilities’ (art 21(c)) and to encourage ‘the mass media, including providers of information through the Internet, to make their services accessible to persons with disabilities’ (art 21(d)).

The above-mentioned States’ obligations laid down at arts 9 and 21 CRPD, which also refer to the accessibility of private services, must be read in light of the general obligations set forth in the Convention. Art 4(1) requires that States take all the appropriate measures to eliminate discrimination on the basis of disability from the part of private entities, such as service providers.¹³ As highlighted by the CRPD Committee in its above-mentioned General Comment on accessibility,

As long as goods, products and services are open or provided to the public, they must be accessible to all, *regardless of whether they are owned and/ or provided by a public authority or a private enterprise*. Persons with disabilities should have equal access to all goods, products and services that are open or provided to the public in a manner that ensures their effective and equal access and respects their dignity. This approach stems from the prohibition against discrimination; denial of access should be considered to constitute a discriminatory act, regardless of whether the perpetrator is a public or private entity.¹⁴

Such prohibition of discrimination also covers information and communication services, as further specified by the CRPD Committee in General Comment No. 6 on equality and non-discrimination.¹⁵ The CRPD ‘indirectly requires ac-

11 CRPD Committee on the Rights of Persons with Disabilities, ‘General comment No. 2’ (n 3), para 13.

12 Rachele Cera, ‘Article 21 [Freedom of Expression and Opinion, and Access to Information]’, in Valentina Della Fina, Rachele Cera and Giuseppe Palmisano (eds), *The United Nations Convention on the Rights of Persons with Disabilities. A Commentary* (Springer 2017), 388.

13 According to the CRPD Committee, however, the lack of accessibility amounts to discrimination against persons with disabilities only if the relevant service has been established after accessibility standards are introduced (CRPD Committee, ‘General Comment No. 2’ (n 3), para 31). According to Broderick and Ferri, the relation between accessibility and discrimination has not been sufficiently clarified by the CRPD Committee. See: Andrea Broderick and Delia Ferri, *International and European Disability Law and Policy. Text, Cases and Materials* (CUP 2019), 149.

14 ‘CRPD Committee, ‘General Comment No. 2’ (n 3), para 13. Emphasis added.

15 CRPD Committee, ‘General Comment No. 6 (2018) on equality and non-discrimination’ (26 April 2018) CRPD/C/GC/6, para 40.

tion at the level of the private sector',¹⁶ by placing accessibility requirements also on the private industry.¹⁷ Nonetheless, it is the primary responsibility of the States Parties to the Convention to make sure that the private sector, including digital services providers, make their services accessible for persons with disabilities, by adopting appropriate legislation and minimum mandatory accessibility standards.¹⁸

General accessibility provisions would be moot if not accompanied by applicable standards. Therefore, besides the above-mentioned accessibility obligations, under the CRPD States are bound to develop standards of accessibility in relation to digital technologies. In particular, art 9(2)(a) CRPD affirms States' duty 'to develop, promulgate and monitor the implementation of minimum standards and guidelines for the accessibility of facilities and services open or provided to the public'. In order to fulfil this obligation, States can delegate the development of technical standards to private, specialized entities. This is what often happens in practice, especially in the digital domain. For instance, the main standardization organization pursuing Internet accessibility is the World Wide Web Consortium (W3C), whose member organizations are universities, NGOs and businesses, including big corporations such as Adobe and Google.¹⁹ The Web Content Accessibility Guidelines (WCAG), developed and periodically reviewed by the W3C, are generally considered the main international standard (currently, in its version 2.1).²⁰

While reliance on ICTs and accessibility specialists can be a valuable instrument for States, based on art 9(2)(a) CRPD, States must take the lead in the standard development process, make standards compulsory and effectively monitor compliance.²¹ At the same time, States' duty to ensure accessibility (also by private entities) is frustrated by the fact that standards, such as the WCAG, are not only developed by private entities, but also mostly of voluntary nature when it comes to the private sector.²² In Italy, for instance, the Stanca Act only

16 Andrea Broderick, 'Of rights and obligations: the birth of accessibility' (n 4), 399.

17 Francesco Seatzu, 'Article 9 [Accessibility]', in Valentina Della Fina, Rachele Cera and Giuseppe Palmisano (eds), *The United Nations Convention on the Rights of Persons with Disabilities. A Commentary* (Springer 2017), 229.

18 CRPD Committee, 'General Comment No. 2' (n 3), paras 27-33.

19 See the list of member organizations: <<https://www.w3.org/Consortium/Member/List>> accessed 15 February 2023.

20 On such private standard, see: Delia Ferri and Silvia Favalli, 'Web Accessibility for People with Disabilities in the European Union: Paving the Road to Social Inclusion', [2018] *Societies* 1, 4-5. The Guidelines are available at: <<https://www.w3.org/WAI/standards-guidelines/wcag/>> accessed 7 February 2023.

21 CRPD Committee, 'General Comment No. 2' (n 3), paras 27-33. See also: Francesco Seatzu (n 17), 228.

22 *ibid.*

imposes web accessibility obligations upon the public sector.²³ It thus depends on the sensitivity of private entities to make their websites and applications accessible.²⁴ Even though it is in the interest of businesses to comply with accessibility requirements – for instance, in terms of corporate image,²⁵ but also to reach a higher number of potential clients –, compulsory standards would strengthen the obligation, making it more effective. In this vein, the CRPD Committee has urged States to adopt mandatory standards, implying sanctions for those who do not comply.²⁶ The importance of ‘effective and enforceable minimum accessibility standards’ has also been stressed in the case law of the CRPD Committee.²⁷

Moreover, in light of the participatory approach embedded in the CRPD’s general obligations,²⁸ and of the interpretation of the Convention provided by the Committee on the Rights of Persons with Disabilities, it is important that also persons with disabilities – through their representative organizations – are given the opportunity to take part in the drafting of national laws, regulations and accessibility standards.²⁹ As underlined by the Committee, ‘the active and informed participation of everyone in decisions that affect their lives and rights is consistent with the human rights-based approach in public decision-making processes, and ensures good governance and social accountability’.³⁰ The idea

23 Legge 9 gennaio 2004, n. 4, Disposizioni per favorire e semplificare l’accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici, GU n. 13 del 17 gennaio 2004, art. 3. On public administration and digital accessibility in Italy, see: Vittorio Pampanin, ‘The Role of Public Administration in Promoting the Accessibility of Online Resources: The Italian Legal Framework’, in Carola Ricci (ed), *Building an Inclusive Digital Society for Persons with Disabilities. New Challenges and Future Potentials* (Pavia University Press 2019).

24 Silvia Favalli, ‘Disability, Social Media and Human Rights: ‘What’s the catch?’ (n 1), 26.

25 See eg the results of EU public consultations with small and medium size enterprises in preparation of the European Accessibility Act (Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services [2019] OJ L151/70): <<https://ec.europa.eu/social/BlobServlet?docId=14843&langId=en>> accessed 4 February 2022, 13-14.

26 CRPD Committee, ‘General Comment No. 2’ (n 3), para 28. See also: Andrea Broderick and Delia Ferri (n 13), 144.

27 Anna Lawson, ‘Article 9: Accessibility’ in Ilias Bantekas, Michael Ashley Stein, Dimitris Anastasiou (eds), *The UN Convention* (n 6), 282. See, in particular: CRPD Committee, *N and T v Hungary* (15 April 2013) CRPD/C/9/D/1/2010; *F v Australia* (16 February 2018) CRPD/C/19/D/19/2014.

28 According to art 4(3) CRPD, States must involve persons with disabilities, through their representative organizations, in the development and implementation of legislations and policies to implement the Convention, and on all decision-making related to persons with disabilities.

29 CRPD Committee, ‘General Comment No. 2’ (n 3), para 48.

30 CRPD Committee, ‘General Comment No. 7 (2018) on the participation of persons with disabilities, including children with disabilities, through their representative organizations, in the implementation and monitoring of the Convention’ (9 November 2018) CRPD/C/GC/7, para 2.

behind States' obligation to seek the participation of the representative organizations of persons with disabilities, including in the drafting of accessibility regulations and standards, is that successful implementation of the CRPD can take place only through constant dialogue with persons with disabilities,³¹ based on the principle 'nothing about us without us'.³² For this reason, according to the CRPD Committee, States Parties should give priority to the views of organizations of persons with disabilities, rather than to civil society in general, when addressing issues directly related to persons with disabilities,³³ including in relation to ICT accessibility.

3. Legal status of the CRPD within the EU legal framework

According to art 44(1) CRPD, regional integration organizations can become a party to the treaty provided that they declare, in the instrument of ratification or accession, the extent of their competence. After having been an active part in negotiations,³⁴ on 30 March 2007, the EC (now EU) signed the CRPD. With Council Decision 2010/48/EC, formally adopted on 26 November 2009 under the former EC Treaty, the Council of the European Union approved the CRPD, authorizing the deposit of the instrument of ratification.³⁵ It is worth noting that the legal basis for the ratification of the CRPD were arts 13 and 95 TCE (now 19 and 114 TFEU),³⁶ dealing, respectively, with non-discrimination and the internal market. Such double legal basis reflects both the founding principle of the European model of protection of the rights of persons with disabilities – namely, the principle of non-discrimination – and the fact that disability is relevant in many areas of EU law.³⁷

Like its Member States, the European Union thus became a party to the CRPD, accessing a human rights treaty for the first time. As noted by Waddington, 'the EU's accession to the CRPD means that the Convention has become a

31 Andrea Broderick and Delia Ferri (n 13), 86-87.

32 *ibid*, 87.

33 CRPD Committee, 'General Comment No. 7' (n 29), para 23.

34 Anna Lawson, 'The European Union and CRPD: Complexities, Challenges and Opportunities', in Valentina Della Fina, Rachele Cera and Giuseppe Palmisano (eds), *The United Nations Convention on the Rights of Persons with Disabilities. A Commentary* (Springer 2017), 61-66.

35 Council Decision of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities, 2010/48/EC, [2010] OJ L23/55.

36 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326.

37 Silvia Favalli, *Disabilità, diritti umani e diritto internazionale* (n 7), 75.

part of EU law, and must be complied with by the EU institutions and legislature'.³⁸ The European Union is not yet a party of the Optional Protocol to the Convention allowing individual petitions to be brought before the Committee on the Rights of Persons with Disabilities, despite the Committee having urged the Union to take such a step.³⁹

Art 216 TFEU establishes that the international agreements that the EU stipulates with other international organizations or third States in its areas of competence are binding upon both the EU and its Member States and form an integral part of EU law. The CRPD amounts to a 'mixed agreement' under EU law, meaning that, in the area of shared competence with Member States – also identified in the EU Declaration annexed to the instrument of ratification⁴⁰ –, the EU has exclusive competence where the Convention affects existing EU provisions that establish common rules, from which the Member States cannot deviate; in contrast, if EU legislation only sets out minimum standards, States remain free to grant stronger protection to persons with disabilities.⁴¹ Also in the latter case, however, the EU can adopt new common rules, if the founding treaties permit it.⁴²

With respect to the rank of the CRPD within the EU legal system, the Convention, like any treaty concluded by the European Union,⁴³ enjoys a lower rank than the primary sources of EU law, but higher with respect to EU secondary legislation.⁴⁴ From the higher rank of the CRPD with respect to EU's secondary legislation, however, it does not follow automatically that the Court of Justice of the European Union (CJEU) can invalidate secondary legislation because in contrast with the Convention. According to the case law of the CJEU, secondary legislation can be reviewed by the Court on the basis of international agreements concluded by the Union only if the treaty provision in question 'contains a clear and precise obligation which is not subject, as regards its implementation or effects, to the adoption of any subsequent measure'.⁴⁵

38 Lisa Waddington, 'The European Union' in Lisa Waddington and Anna Lawson (eds), *The UN Convention on the Rights of Persons with Disabilities in Practice. A Comparative Analysis of the Role of Courts* (OUP 2018), 131.

39 CRPD Committee, 'Concluding observations on the initial report of the European Union' (2 October 2015) CRPD/C/EU/CO/1, paras 6-7.

40 <https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-15&chapter=4&clang=_en#EndDec> accessed 9 February 2023.

41 Lisa Waddington, 'The European Union and the United Nations Convention on the Rights of Persons with Disabilities: A Story of Exclusive and Shared Competences' [2011] *Maastricht Journal of European and Comparative Law* 431, 445-446.

42 Ibid.

43 See: Luigi Daniele, *Diritto dell'Unione europea* (6th edn, Giuffrè 2018) and the case law mentioned therein.

44 Lisa Waddington, 'The European Union' (n 38), 138.

45 Case C-93/02 P *Biret International SA v Council of the European Union* [2003] ECR I-10497 para 60. See also, eg: Case C-213/03 *Pêcheurs de l'étang de Berre* [2004] ECR I-07357, para 39.

This is not, however, the case of the CRPD. In a case concerning surrogacy birth and maternity leave, the CJEU clarified that the Convention has no direct effect on EU law, precisely because its provisions ‘are not, as regards their content, provisions that are unconditional and sufficiently precise’.⁴⁶ According to the Court, it is apparent from art 4(1) of the CRPD, concerning general obligations, ‘that it is [...] for the States Parties to adopt all appropriate legislative, administrative and other measures for the implementation of the rights recognised in that Convention’.⁴⁷

Still, as affirmed in the case law of the Court of Justice of the European Union, the primacy of the international treaties to which the Union is a party over EU secondary legislation implies that the latter must be interpreted in a manner which is as far as possible consistent with those international agreements.⁴⁸ Therefore, EU secondary legislation must be interpreted in a manner which is, as far as possible, consistent with the provisions of the CRPD.⁴⁹

Assessing EU’s secondary legislation based on the obligations enshrined in the CRPD, to which the European Union is bound as concerns its areas of competence, is very important from a reform perspective. Therefore, the next two paragraphs will be dedicated to the analysis of EU legislative instruments dealing with the accessibility of ICTs, which were adopted by the European Union following ratification of the CRPD.

4. Binding EU instruments on accessibility: the Web Accessibility Directive and the European Accessibility Act

Few Member States of the European Union had adopted binding accessibility requirements for both the public and the private sector before the EU introduced accessibility obligations in its areas of competence.⁵⁰ The two main

46 Case C-363/12 *Z v A Government department, The Board of management of a community school* [2014] ECR 159, para 90.

47 *ibid*, para 87.

48 See eg: Case C-61/94 *Commission v Federal Republic of Germany* [1996] ECR I-03989, para 52; Joined Cases C-288/09 and C-289/09 *British Sky Broadcasting Group* [2011] ECR I-02851, para 83; Joined Cases C-320/11, C-330/11, C-382/11 and C-383/11 *Digitalnet* [2012] ECR 745, para 39; Case T-527/14 *Rosenich v EUIPO* [2012] ECR 487, para 54.

49 See eg: Joined Cases C-335/11 and C-337/11 *Ring and Werge* [2013] ECR 222, para 32; Case C-824/19 *TC and UB* [2021], para 59. On the interpretation of the EU secondary legislation in line with the CRPD, see: Lisa Waddington, ‘The European Union’ (n 38), 143-150.

50 ANED, ‘National accessibility requirements and standards for products and services in the European single market: overview and examples Compiled by Mark Priestley on behalf of the Academic Network of European Disability experts (ANED)’ (January 2013) <<https://ec.europa.eu/social/BlobServlet?docId=14840&langId=en>> accessed 9 February 2023.

legislative instruments adopted by the Union, dealing specifically with ICTs accessibility, are the Web Accessibility Directive⁵¹ and the European Accessibility Act.⁵² The objective of EU accessibility legislation is not only to ensure respect of the CRPD, but also to expand the single market by making more products accessible and to promote interoperability among Member States, making cross-border trading easier.⁵³ The market-oriented nature of this legislation is clear from its legal basis, which is art 114(1) TFEU, concerning the internal market.

With the 2016 Directive on web accessibility the EU set out minimum harmonization requirements for public sector bodies. All Member States have adopted the necessary domestic legislation,⁵⁴ but problems in the accessibility of websites and mobile applications of public bodies still remain.⁵⁵ The Directive also encourages States to extend accessibility standards to private entities which offer services to the public,⁵⁶ but does not impose binding obligations upon private entities. A further limitation is that the Directive excludes from its scope of application the websites and applications of public broadcasters and to the websites and applications of NGOs which are deemed not to provide essential services for the public.⁵⁷ The 2016 Directive has thus a limited scope of application.⁵⁸

Following the recommendation of the CRPD Committee to adopt a comprehensive accessibility act,⁵⁹ binding obligations upon private entities were introduced with the 2019 EU Accessibility Act. Differently from the 2016 Web Accessibility Directive, the European Accessibility Act regulates both the public and private sector, imposing obligations upon the providers of certain services that are considered of major importance for people with disabilities, such as computers and operating systems, smartphones, e-books, banking services,

51 Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies [2016] OJ L327/1.

52 Directive (EU) 2019/882 (n 25).

53 See, eg, the presentation of EU accessibility legislation on the website of the EU Commission: <<https://ec.europa.eu/social/main.jsp?catId=1202>> accessed 15 February 2023.

54 For instance, in Italy the Web Accessibility Directive has been implemented by means of d.lgs. 10 agosto 2018 n. 106, GU 211 dell'11 settembre 2018, amending the aforementioned *Legge Stanca* and the so-called codice dell'amministrazione digitale, namely d.lgs. 7 marzo 2005, n. 82, GU n. 112 del 16 maggio 2005.

55 See, eg, the Study supporting the review of the application of the Web Accessibility Directive, commissioned by the EU Commission: <<https://digital-strategy.ec.europa.eu/en/library/study-supporting-review-web-accessibility-directive>> accessed 15 February 2023.

56 Directive (EU) 2016/2102 (n 51), recital n 34.

57 *ibid*, art 1(3).

58 For critical remarks, see: Delia Ferri and Silvia Favalli (n 20), 11.

59 CRPD Committee, 'Concluding observations on the initial report of the European Union' (n 39), paras 28-29.

ticketing and ticket machines, e-commerce, transport related services, emergency communications.⁶⁰ The Directive sets forth obligations for a wide range of private entities, including manufacturers, representatives, importers and distributors. Like the Web Accessibility Directive, the European Accessibility Act aims not only to comply with the accessibility obligations enshrined in the CRPD,⁶¹ but to improve the functioning of the internal market by removing barriers created by divergent rules in Member States.⁶² Member States had to adopt the laws, regulations and administrative provisions necessary to comply with this Directive by June 2022. To date, nine States failed to report on the measures adopted.⁶³ Private companies shall conform to those new national regulations from 28 June 2025.⁶⁴

The European Accessibility Act presents a number of shortcomings. Firstly, microenterprises are excluded from its scope of application,⁶⁵ which implies that enterprises with less than ten employees do not need to make their services accessible. Secondly, the obligations enshrined in the European Accessibility Act are to be complied with by private enterprises only if there is no excessive financial burden.⁶⁶ This provision can be criticized on the ground that considerations of burden proportionality are entailed by the concept of reasonable accommodation, but are not proper to the principle of accessibility, which must be realized to the maximum extent.⁶⁷ Moreover, the assessment of what represents a financial burden is primarily left to the self-assessment of the industry,⁶⁸ even if national surveillance authority must review companies' assessments,⁶⁹ based on specific criteria set out in an annex to the European Accessibility Act.⁷⁰ However, despite its above-mentioned shortcomings and market-oriented nature, the European Accessibility Act can be regarded as a positive example of legislation that implements the duties enshrined in the CRPD through the imposition of binding web accessibility obligations upon the private sector.

60 Directive (EU) 2019/882 (n 25), art 2.

61 *ibid*, recitals n 15-16.

62 *ibid*, recital n 1.

63 <<https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32019L0882>> accessed 9 February 2023.

64 Directive (EU) 2019/882 (n 25), art 2.

65 *ibid*, recital n 70.

66 *ibid*, art 14 and recitals n 66-67.

67 Andrea Broderick, 'The European Accessibility Act: A Paradigm of Inclusive Digital Equality for Persons with Disabilities?', in Carola Ricci (ed), *Building an Inclusive Digital Society for Persons with Disabilities. New Challenges and Future Potentials* (Pavia University Press 2019), 30.

68 This was a critical element already in the Draft European Accessibility Act, as highlighted by the NGO Inclusion Europe, a representative organization of persons with disabilities: <https://inclusion-europe.eu/wp-content/uploads/2015/03/IE_policypaper_EAA_final.pdf> accessed 15 February 2023, 6. See also Delia Ferri and Silvia Favalli (n 20), 13.

69 Directive (EU) 2019/882 (n 25), art 19.

70 *ibid*, Annex VI.

With respect to standards of accessibility, following the adoption of the 2016 Web Accessibility Directive, the EU Commission adopted an implementing decision requesting European standardization organizations⁷¹ – composed by one member association per Member State, often amounting to partnerships between the private and the public sectors – to set a technical standard in accordance with the Directive.⁷² This standard has recently been updated to be in line with the more recent WCAG (WCAG 2.1).⁷³ As of today, however, this standard is compulsory only for public sector bodies, as it is linked to the Web Accessibility Directive, but not to the European Accessibility Act. The latter only sets out functional requirements of accessibility, without specifying how they are to be implemented from a technical point of view.⁷⁴ According to commentators, including the European Disability Forum – an umbrella organization representing persons with disabilities –, this is a positive aspect because it leaves a certain flexibility to the private sector, possibly fostering technological innovations.⁷⁵

With respect to the participatory model which, according to the general obligation enshrined in art 4(3) CRPD, State Parties must adopt when designing regulations and policies which affect persons with disabilities, the Commission opened consultations with the public in general, including persons with disabilities and their representative organizations, before and after the adoption of e-accessibility legislation. A recent example is the public consultation on the 2016 Web Accessibility Directive, aimed at evaluating the impact of the legislation and at identifying its possible gaps and weaknesses.⁷⁶ Another example is the public consultation opened before the adoption of the European Accessibility Act.⁷⁷ In this case, however, besides a general consultation, a specific one was opened with respect to small and medium enterprises, rather than with the organizations representing persons with disabilities, which makes even

71 CEN, CENELEC and ETSI.

72 Commission Implementing Decision C(2017)2585 of 27 April 2017 on a standardisation request to the European standardisation organisations in support of Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies [2017] OJ L327/84.

73 Commission Implementing Decision (EU) 2021/1339 of 11 August 2021 amending Implementing Decision (EU) 2018/2048 as regards the harmonised standard for websites and mobile applications [2021] OJ 289/53.

74 Directive (EU) 2019/882 (n 25), Annex I.

75 Delia Ferri and Silvia Favalli (n 20), 13.

76 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12537-Accesible-web-&-digital-content-for-people-with-disabilities-review-of-EU-rules/public-consultation_en> accessed 15 February 2023.

77 Deloitte, ‘Study on the socio-economic impact of new measures to improve accessibility of goods and services for people with disabilities. Public Consultation Analysis’ <<https://ec.europa.eu/social/BlobServlet?docId=14842&langId=en>> accessed 9 February 2023.

more apparent the market-oriented nature of the legislation.⁷⁸ As to monitoring, persons with disabilities are involved, through the participation of their representative organizations, in the working group which monitors and facilitates compliance with the European Accessibility Act.⁷⁹ The action of the Union with respect to the involvement of persons with disabilities into the design and review of legislation on ICT accessibility can thus be positively evaluated, even though it could be further improved by granting more targeted participation of persons with disabilities.

5. The EU Digital Services Act: a critical assessment

Always at the level of EU secondary legislation, the Union recently adopted the Digital Services Act. The Regulation entered into force twenty days after its publication on the official journal and will apply from 17 February 2024. The Digital Services Act regulates digital platforms which offer intermediary services (including search engines), complementing the Digital Markets Act. The Digital Services Act focuses on the removal of illegal content online, also by allowing users to signal illegal content (art 16). It also establishes due diligence obligations for a transparent and safe online environment, including, for instance, transparent terms and conditions related to the policies for content moderation and redress mechanisms (art 14), and transparency reporting obligations, for instance on the removed content (art 15).

As apparent, differently from the Web Accessibility Directive and the European Accessibility Act, the Digital Services Act does not deal specifically with digital accessibility. It does contain, however, relevant provisions on e-accessibility, which have been so far neglected by commentators, except by organizations representing persons with disabilities.⁸⁰ The present section will thus discuss the DSA and its legislative history precisely in the light of the rights of persons with disabilities.

In its first reading of the Commission's proposal for the Digital Services Act, the European Parliament had voted in favour of an amendment introducing an accessibility obligation for online platforms. In particular, art 19(a) of the

⁷⁸ Deloitte, 'Analysis of the results of the SME Panel consultation on the socio-economic impact of new measures to improve the accessibility of goods and services for people with disabilities' <<https://ec.europa.eu/social/BlobServlet?docId=14843&langId=en>> accessed 9 February 2023.

⁷⁹ Directive (EU) 2019/882 (n 25), art 28. On the participative dimension of the European Accessibility Act, see: Andrea Broderick, 'The European Accessibility Act' (n 67), 32-33.

⁸⁰ See, eg, the position of the European Disability Forum: EDF, 'Digital Services Act fails to ensure accessibility for persons with disabilities. EDF calls the EU to rectify this political agreement' (10 May 2022) <<https://www.edf-feph.org/digital-services-act-fails-to-ensure-accessibility-for-persons-with-disabilities-edf-calls-the-eu-to-rectify-this-political-agreement/>> accessed 14 March 2023.

amended regulation obliged platforms which offer services in the Union to ensure that they design and provide services in accordance with the accessibility requirements set out in the European Accessibility Act.⁸¹ With this amendment, the DSA would have extended the list of private entities bound to comply with a mandatory accessibility standard for ICTs under EU legislation, thus complementing and strengthening the protection of the rights of persons with disabilities enshrined in the European Accessibility Act, and ensuring better compliance with the CRPD. Unfortunately, however, such provision was not included in the final text of the Digital Services Act negotiated with the Council, raising the protests of the associations representing persons with disabilities, which had lobbied in favour of mandatory accessibility requirements for digital platforms.⁸² This result might be due also to the fact that a general consultation was launched with regard to the Digital Services Act, but with no specific focus on persons with disabilities.⁸³

The Digital Services Act in its final version does not provide for an obligation for online platforms to ensure accessibility for persons with disabilities, but makes accessibility a matter of voluntary codes of conduct to be adopted by providers. Based on art 47 of the Digital Services Act, and as reflected in recital n 105 of the Preamble, the European Commission shall encourage and facilitate the drawing up of codes of conduct on accessibility for persons with disabilities, with the participation of providers of online platforms and other relevant service providers, as well as of organisations representing persons with disabilities and civil society organisations or relevant authorities.⁸⁴ The Commission ‘shall aim to ensure that the codes of conduct pursue the objective of ensuring that those services are accessible in compliance with Union and national law, in order to maximise their foreseeable use by persons with disabilities’, by making services perceivable, operable, understandable and robust – as prescribed by the aforementioned WCAG standard –, and by making information on how they meet the accessibility requirements accessible and easy to find for persons with disabilities.⁸⁵ The codes of conduct shall be developed by 18 February 2025 and applied by 18 August 2025.⁸⁶

81 Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825), P9_TA(2022)0014, Amendment 255: <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html> accessed 15 March 2023.

82 EDF, ‘Digital Services Act’ (n 80).

83 Summary Report on the open public consultation on the Digital Services Act Package (15 December 2020) <<https://digital-strategy.ec.europa.eu/en/library/summary-report-open-public-consultation-digital-services-act-package>> accessed 9 February 2023.

84 Regulation (EU) 2022/2065 (n 5), art 47(1).

85 *ibid*, art 47(2).

86 *ibid*, art 47(3).

The compromise solution reached by the European Parliament and the Council has been harshly criticized by the associations representing persons with disabilities. According to the European Disability Forum, by leaving accessibility measures to the goodwill of service providers, the Council and Parliament ‘instead of owning up to their commitments under the CRPD and ensuring a rights-based approach to disability inclusion, [...] opted for a charity-based approach’.⁸⁷ In the Forum’s view, the Digital Services Act leaves persons with disabilities in a position of vulnerability, because, besides not being able to fully access online services, they will not enjoy as a matter of rights the protection granted by the Digital Services Act, for instance in terms of data protection.⁸⁸ The underlying idea is that human rights, including the rights of persons with disabilities, are fully respected, protected and realized only through binding rules associated with appropriate enforcement mechanisms. Albeit founded, this criticism must be contextualized in the light of both States’ obligations enshrined in the CRPD in matters of accessibility, and the functions pursued by codes of conduct.

Codes of conduct can be defined as ‘regulatory instruments consisting of written sets of rules which can deal with very specific or more general areas of regulatory concern, but always focus on a certain desirable conduct of the addressee’.⁸⁹ A typical feature of codes of conduct is that they are non-binding, although they might reflect (or specify) binding rules.⁹⁰ They can be classified based on source and addressee,⁹¹ ranging from guidelines developed at the international level and addressed to States, to the self-regulatory codes of conduct adopted by private entities.⁹² At the European Union level, codes of practices developed by and for private entities have been regarded as useful initiatives at least since 2003, as reflected in the inter-institutional agreement on better law-making adopted by the European Parliament, the Council and

87 EDF, ‘Digital Services Act’ (n 80).

88 *ibid.* On data protection and privacy concerns with a focus on persons with disabilities, see: Silvia Favalli, ‘Disability, Social Media and Human Rights: “What’s the catch?”’ (n 1), 30-34.

89 Jürgen Friedrich, ‘Codes of Conduct’ in Rüdiger Wolfrum (ed), *The Max Planck Encyclopedia of Public International Law* (vol II, OUP 2012), 264.

90 *ibid.*, 265.

91 See the categorizations made in Jürgen Friedrich (n 89) and Fabrizio Marrella, ‘Regolazione internazionale e responsabilità globale delle imprese transnazionali’, [2009] *Diritti umani e diritto internazionale* 229, 242-254.

92 The two opposite sides of the spectrum might, however, influence each other. On the interrelation between international soft law and the self-regulatory standards developed by private entities, with a focus on food law, see: Carola Ricci, ‘Circolazione di standard internazionali di sicurezza alimentare: quando regolatore pubblico e privato si confondono’, in Elisabetta Colombo (ed), *Le istituzioni e le idee. Studi indisciplinati offerti a Fabio Rugge per il suo settantesimo compleanno* (Giuffrè 2022).

the Commission that year.⁹³ Codes of conduct, whose development is often foreseen by EU secondary legislation (as in the case of the Digital Services Act), have become veritable co-regulatory instruments voluntarily adopted by the private sector, but with the facilitation of the European Commission (and possibly, also of other EU and national institutions). Relevant examples include, for instance, codes of conduct under the General Data Protection Regulation (GDPR),⁹⁴ and the EU code of conduct on responsible food business and marketing practices.⁹⁵ The same Digital Services Act delegates to codes of conduct the regulation not only of digital accessibility, but also of online advertising.⁹⁶

Despite their non-binding character, and as evinced by their widespread adoption at international and national level, codes of conduct addressed to private entities are not necessarily ‘the enemy’ of human rights. Codes of conduct and guidelines adopted at the inter-State level serve the useful function to regulate, at least in a non-binding form, the conduct of enterprises in absence of agreement among States.⁹⁷ Likewise, at the European Union level codes of conduct developed by private parties through dialogue with EU institutions have been used, in absence of appropriate legal basis for EU legislation or in case of disagreement among Member States, to convince private actors to grant higher standards of conduct than those embedded in binding national or EU legislation.⁹⁸ Although effectiveness overall remains a matter of discussion,⁹⁹ codes of conduct enjoy a high compliance rate when they are elaborated directly by the addressed economic sector, or in close coordination with it.¹⁰⁰ In fact, private entities follow codes of conduct in order to be labelled as respecting a certain ethics and/or quality standard: therefore, for their own economic

93 Interinstitutional agreement on better law-making of 16 December 2003, 2003/C 321/01 [2003] OJ C321/1. Codes of conduct for the private sector must be distinguished from the self-regulatory codes adopted by EU institutions. On the subject, see: Paola Mori, ‘La codificazione del diritto dell’Unione europea e i suoi strumenti’, [2019] *Il diritto dell’Unione europea* 109, 132-133.

94 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016] OJ L119/1, art 40.

95 EU Code of Conduct on Responsible Food Business and Marketing Practices (June 2021) <https://food.ec.europa.eu/horizontal-topics/farm-fork-strategy/sustainable-food-processing/code-conduct_en> accessed 4 April 2023.

96 Regulation (EU) 2022/2065 (n 5), art 46.

97 Francesco Salerno, ‘Natura giuridica ed effetti dei codici di condotta internazionali per le imprese multinazionali’ [2005] *Lavoro e diritto* 655, 657.

98 Oreste Pollicino, ‘I codici di condotta tra *self-regulation* e *hard law*: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online’ [2022] *Rivista trimestrale di diritto pubblico* 1051, 1058.

99 Jürgen Friedrich (n 89), 269.

100 Fabrizio Marrella (n 91), 248.

interest.¹⁰¹ Moreover, codes of conduct might act as catalyst for the adoption of binding rules.¹⁰²

Codes of conduct regulating digital accessibility for persons with disabilities like those foreseen by art 47 of the Digital Services Act, ie developed directly by the service providers with the facilitation of the EU Commission, might thus help improving accessibility for persons with disabilities, especially if service providers think that they might get economic advantages by extending their user base. Leaving accessibility regulation only to codes of conduct, however, does not fully comply with States' obligation to 'ensure that private entities that offer facilities and services which are open or provided to the public take into account all aspects of accessibility for persons with disabilities', laid down in art 9(2)(b) CRPD. While private standards can be very useful to promote digital accessibility – as the WCAG standard demonstrates –, based on the CRPD's provisions on accessibility and the interpretation provided by the Committee,¹⁰³ States must set out at least minimum accessibility obligations for private service providers. Such obligations could then be better specified, if needed, in codes of conduct, which cannot, however, be the only source of regulation on accessibility. We thus agree with the European Disability Forum's criticism whereby the Digital Services Act is a missed opportunity which, instead of building on the European Accessibility Act, 'takes Union accessibility policy a step back'.¹⁰⁴

6. Conclusive remarks

The European Union has taken significant – albeit limited – steps to ensure digital accessibility for persons with disabilities with the adoption of the Web Accessibility Directive and, three years later, of the European Accessibility Act. Unfortunately, the regulation of accessibility through voluntary codes of conduct set forth in the Digital Services Act is not sufficient to ensure full compliance with EU's international obligations under the CRPD, nor does it realise the promise of a truly inclusive digital environment in the Union. Hopefully, the rights of persons with disabilities will be better mainstreamed in future EU legislation and policy through the systematic involvement of persons with disabilities and their representative organizations. The newly established European Disability Platform, a flagship initiative of the EU Disability Strategy 2021-2030, might be an opportunity in this respect.¹⁰⁵

101 In this sense, see eg: Francesco Galgano and Fabrizio Marrella, *Diritto del commercio internazionale* (3rd edn, CEDAM 2011), 926-927.

102 Jürgen Friedrich (n 89), 270.

103 CRPD Committee, 'General comment No. 2' (n 3), para 13.

104 EDF, 'Digital Services Act' (n 80).

105 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Union of Equality: Strategy for the Rights of Persons with Disabilities 2021-2030', 3 March 2021, COM(2021) 101 final.

The Digital Services Act and the Regulation on the Transparency and Targeting of Political Advertising: Initial Reflections

Pietro Villaschi

University of Milan, Italy

ORCID 0000-0001-7166-9850

DOI: 10.54103/milanoup.215.c462

Abstract

This paper analyses the issue of the manipulation of political consensus on social media and the impact of this phenomenon on the resilience of democratic systems. After highlighting characteristics and consequences of political targeting, the Author reflects on the regulations recently approved by the European Union, in particular the Digital Services Act and the Regulation on the transparency and targeting of political advertising. The aim is to point out opportunities and criticalities of the strategy developed by the European Union to meet the challenges of the digital revolution.

Keywords

Targeting; Political Propaganda; Digital Revolution

1. Introduction

At the time of ‘surveillance capitalism’,¹ the use of targeting for the purposes of building and manipulating political consensus plays a key role in influencing public opinion. This is particularly true during election campaigns, where massive profiling can influence the outcome of the elections. Indeed, consensus-building on social media by candidates and political parties is characterized by sending marked oriented messages to selected groups of voters in order to find their preferences.²

1 S Zuboff, *The age of surveillance capitalism: the fight for the future at the new frontier of power* (Faber faber 2019) 1ff.

2 See F Balaguer Callejon, *La Constitució del algoritmo* (Fundació Manuel Gimenez Abad 2023), 1ff.

Targeting, which is one of the most significant differences between online communication and traditional broadcasting, affects the right of citizen-voters-users to be informed and the principle of media pluralism, which, as the Italian Constitutional Court has pointed out, is a prerequisite for the functioning of the democratic system.³

Therefore, the use of these practices, which fosters an increasingly disintermediated relationship between voters and representatives, has a rebound effect on the party-political system, encouraging the rise of charismatic leaders, who take their strength and legitimacy from unfiltered communication.

More generally, there are consequences on the democratic system, in terms of the quality of public discourse, of the ability of citizens to form their own ideas and, ultimately, of the outcome of the elections.

After giving a brief overview of the characteristics and consequences of online political communication, this paper analyses the last regulations adopted by the European Union. The reference is to the ‘Digital Services Act’⁴, the regulation on digital services, published on 27 October 2022, which, together with the ‘Digital Markets Act’⁵, constitutes one of the founding pillars of the ‘Digital Services Package’, and to the last ‘Regulation on the transparency and targeting of political advertising’⁶, recently approved on 13 March 2024.

These regulations constitute a first significant response to the issue of limiting the powers of internet platforms as well as guaranteeing users’ rights in the EU internal market.

2. The impact of online profiling and targeting

The rise of social media had raised high hopes about the democratic potential of communication tools capable of decentralizing the production and consumption of political messages and fostering dialogue among users. The literature considered that ICTs would have the potential to cure the dysfunctions of modern democracies, reviving citizens’ involvement in political life, fostering the free circulation of ideas, and giving rise to new deliberative spaces. Social media were appreciated for their ability to stimulate communication with no

3 M Monti, ‘Le Internet platforms, il discorso pubblico e la democrazia’ (2019) 4 Quaderni costituzionali 811, 811ff.

4 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277.

5 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265.

6 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L, 2024/900.

space-time barriers. The use of the Internet was imagined to be pluralist, open and free, like no other communicative space experienced until then.⁷

However, this scenario was belied by the facts. Interaction on social networks has been developing on the basis of algorithms which produce dynamics completely at odds with the most elementary deliberative principles: there are mechanisms which profile and segment the public on the basis of preferences of users; which encourage the meeting of similar opinions, reinforcing previous convictions (and related prejudices) and penalizing the comparison between different points of view; which allow for the selection of message recipients and, therefore, allow the same subject to address different and incoherent messages to portions of the electorate; which encourage the circulation of fake news; which give rise to the computational propaganda, ie the manipulation of public opinion online through political micro-targeting and bots/trolls in order to distribute automated political messages on social media; which enable disintermediated forms of communication and a hyper-personal relationship between representatives and voters.⁸

In order to understand this phenomenon, it should be considered that profiling, even before the political sphere, has been widely used for commercial purposes to show users products and services that the algorithm considers to be consistent with their profiles, going so far as to guide and condition the choices of the consumer, who is not exposed in this way to alternative products and services, but only to those that are deemed more attractive to him. Profiling is configured as a strategic process directed to influence the public through messages, based on the preferences of each user, to show the final consumer the product that should arouse the greatest interest and appreciation.⁹

As long as this process is limited to the sphere of private interests and the field of commercial advertising, it does not raise concerns. When, however, the same mechanism is placed at the service of the commercialization of the political message, being able to influence the political and even electoral orientation of users, the evaluation changes.

Three effects are interesting for the constitutional law.

Firstly, profiling affects protection of users' personal data, given the fact that the algorithms used for this purpose essentially feed on data, the processing of which is often authorized in the absence of a real awareness that some services,

7 See P Lévy, *Le tecnologie dell'intelligenza. L'avvenire del pensiero nell'era informatica?* (ES/Synergon 1992), 76 ff; D De Kerckhove, A Tursi (eds), *Dopo la democrazia. Il potere e la sfera pubblica nell'era delle reti* (Apogeo 2006) 13ff.

8 See T Dobber, R Fathaigh and F Zuiderveen Borgesius, 'The regulation of online political micro-targeting in Europe' (2019) 8(4) *Internet Policy Review* 1, 5ff; A Floridia, 'La rete, la sfera pubblica e i luoghi della deliberazione pubblica' (2014) 2 *Iride* 319.

9 See K Klonic, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598, 1599ff.

apparently proposed as free by the platforms, conceal a commercialization of personal data.¹⁰

Secondly, profiling tends to isolate the user within filter bubbles, in which there is a reinforcement of initial positions and related prejudices, instead of a critical confrontation with other ideas, which become invisible on the web, even though they exist. As a result, there is a strong cyber-polarization of public discourse, as users hear nothing but the amplified echo of their own voice.¹¹

Political-electoral profiling also affects the role of political parties, both in terms of their relationship with the voters and the 'new intermediaries' of the digital society. Firstly, such techniques can be very expensive, favoring parties with greater financial resources. Secondly, such practices allow candidates to shape their image according to the daily expectations of the electorate. Moreover, since some users are not very active online, parties could base their political campaign only on the analysis of data provided by users who make more frequent use of social media.¹²

Third, these activities take place in a context of media disintermediation. The network has allowed anyone to search for information, but also to produce and share it, exponentially increasing the number of information sources.¹³ This absence of mediation, however, causes a strong personalization of the political and party system: leaders use targeting to build a direct and unfiltered communication with their voters, which favors the rise of political parties by real 'outsiders', who prove to be much more adept than professional politicians at communicating with the electoral base.

Finally, targeting techniques result in the fragmentation of public opinion into closed and polarized groups.¹⁴ The combined effect of fake news, cyber-cascades and confirmation bias tends to alter the perception of the real relevance of issues, affecting freedom of information and, in particular, the right to be informed, which, as the Constitutional Court has recognized, 'must be determined and qualified with reference to the founding principles of the form of State outlined by the Constitution, which require that our democracy be based on free public opinion and be able to develop through the equal competition of all in the formation of the general will'.¹⁵

10 See G D'Ippolito, 'Comunicazione politica online: dal messaggio politico commercializzato alle sponsorizzazioni sui social network' (2020) 1 MediaLaws 159, 167ff.

11 C R Sunstein, *Repubblic.com. Cittadini informati o consumatori di informazioni?* (Il Mulino 2001) 1ff.

12 See M Calise, 'Il destino dei partiti' (2023) 1 Quaderni costituzionali 101, 101ff.

13 Floridia (n 8) 324.

14 See A Cardone, «Decisione algoritmica» vs decisione politica? *A.I. Legge. Democrazia* (Editoriale scientifica 2021), 72ff.

15 Constitutional Court, sent. 112/1993, para 7.

Therefore, the regulation of these processes is necessary, to avoid a pathological distortion of political representation and participation to democratic processes.

3. The European Union's change of approach

After a long period in which, despite the absolute relevance of this phenomenon, the self-regulation of the platforms had prevailed and users had the alternative between accepting profiling and the commercialization of their personal data or not accessing the service of online platforms, the European Union has changed its regulatory approach.

Among the most significant measures adopted, we find the Regulation (EU) 2022/2065 on a single market for digital services, well known as the Digital Services Act (DSA), which, after a long legislative process, was finally published on 27 October 2022. The regulation, which came into force the following 16th November, is directly applicable in all EU States from 17 February 2024. Together with the Digital Markets Act, which was approved a few weeks earlier and which aims to ensure competition in the internal market for digital services, it constitutes one of the pillars of the Digital Services Package, the strategy put in place by the European institutions to ensure a predictable and reliable digital space.

With this regulation, the European legislator aims to harmonize the rules applicable to intermediary services in the internal market. From a subjective point of view, the DSA applies to 'intermediary service providers' (whether mere conduit, caching or hosting), ie all those entities which provide 'any service, normally for remuneration, at a distance, by electronic means and at the individual request of a recipient'.

In particular, the regulation provides:

(a) some general provisions, which apply to all service providers irrespective of their respective characteristics (section I, arts 11–15);

(b) additional provisions concerning hosting service providers, including online platforms (section II, arts 16–18);

(c) a set of provisions relating exclusively to online platform providers (section III, arts 19–28);

(d) additional provisions, which apply to those online platform providers that allow consumers to conclude distance contracts with traders (section IV, arts 29–32);

(e) finally, additional obligations for very large platforms and search engines (section V, arts 33–44). Very large platforms and search engines (VLOPs and VLOSEs respectively) are those entities, which have an average monthly number of active users of 45 million or more in the EU. Recognition takes place

following a procedure, governed by Article 33 of the Regulation, which ends with an EU Commission statement.

First of all, the DSA – incorporating the recommendations that had been formulated by the European Data Protection Board (EDPB) in relation to the risks of targeting to which users are subjected and of circumventing the provisions relating to the GDPR – at art 26 establishes that providers of online platforms shall ensure that, for each and every advertisement, the recipients of the service are able to identify clearly, concisely and unequivocally: (a) that the information constitutes an advertisement, including through visible markings; (b) the natural or legal person on whose behalf the advertisement is presented or paid for; (c) the relevant information relating to the parameters used to determine the recipient of the advertisement and, where applicable, how those parameters can be changed by the user.

Furthermore, online platform providers must make available to the recipients of the service a functionality allowing them to declare whether the content they provide contains commercial communications. Concerning the transparency, art 27 provides that online platform providers, who make use of recommender systems, must specify, in their general terms and conditions, in clear and intelligible language, the main parameters used, as well as any option available to the recipients of the service, that allows them to change these parameters. In addition, providers of online platforms must also make available a functionality enabling the recipient to select and modify, at any time, the preferred option relating to the parameters by which advertisements are determined.

With regard, on the other hand, to the data that may or may not be subject to profiling, art 26 establishes an (absolute) ban on presenting advertising to service recipients based on the profiling of the special categories of personal data referred to in Article 9(1), of the GDPR. It follows that platforms will no longer be able to profile users by using data relating, for example, to racial or ethnic origin, to political opinions, to religious or philosophical beliefs, to trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data relating to health or sex life or sexual orientation. This provision should be read in conjunction with art 28 of the DSA, which also prohibits advertising based on personal data of service users who are minors.

Additional obligations are foreseen for very large platforms and search engines (VLOPs and VLOSEs), which are, first and foremost, required to identify, analyze, and assess any systemic risks arising from the design or operation of their service and systems, including algorithmic systems (arts 34–35).

Above all, there are two provisions that are important for the purposes of this analysis. Art. 38 stipulates that, in addition to the requirements of art 27 mentioned above, VLOPs and VLOSEs shall ensure the user at least one option for their recommendation systems that is not based on profiling. Art 39 provides that all very large platforms, which present advertisements on their online

interfaces, shall compile and make available to the public, in a specific section of their online interface, a register containing a series of information for the entire period during which they present the advertisement. This register shall necessarily set out: (a) the content of the advertisement, including the name of the product, service, trademark and the subject matter of the advertisement; (b) the natural or legal person on whose behalf the advertisement is presented or paid for; (c) the period during which the advertisement is presented; (d) an indication of whether the advertisement was intended to be presented to one or more specific groups of addressees of the service and, if so, the main parameters used for that purpose; (e) the commercial communications published; (f) the total number of addressees of the service reached and aggregate data broken down by Member State for the group or groups of addressees to which the advertisement was specifically addressed.

These obligations witness a change of approach of the European Union. Faced with the failure of self-regulation, the European institutions have chosen to intervene, for the first time, with a regulation and not with soft-law.¹⁶ The regulation is wide-ranging and constitutes one of the most significant novelties a few years after the ‘foundation pillar’ of the European protection of users’ digital rights, ie the GDPR.

In particular, the decision to indicate on whose behalf and with what parameters advertisements are presented to users is positive, as well as the provision that prohibits profiling from taking place based on special categories of data pursuant to Article 9 GDPR or on data concerning minors. This novelty mainly follows the recommendations pointed out by the doctrine, which had highlighted how platforms substantially circumvent the GDPR, which merely required explicit consent for the processing of such categories of data. Indeed, this provision, obliging very large platforms to offer at least one recommendation system that is not based on profiling, is significant: as a result, online platforms must provide users with at least one non-profiling-based mode.

However, some doubts and questions arise.

First, the measures discussed above apply only to hosting providers and not to all data controllers, so that some providers may be excluded. Secondly, it is difficult to define exactly the perimeter of the ‘special category of data’ under art 9 GDPR and, therefore, which information cannot be profiled also due to the DSA. This demonstrates that the regulation of these phenomena is not

16 See C Frisani, ‘Il Digital Services Act: le prospettive di riforma per una maggior tutela online’ (*Ius in itinere*, 2022) 1ff.; O Grandinetti, ‘Le piattaforme digitali come “poteri privati” e la censura online’ (2022) 4(1) *Rivista italiana di informatica e diritto* 175, 175ff; G Tiberi, ‘L’irresistibile ascesa della sovranità digitale europea’ in G Ferri (eds.), *Diritto e nuove tecnologie* (ESI 2022), 175–216.

easy and that the online platforms, even in the presence of stricter rules, could circumvent the prohibitions laid down by the EU legislator with the DSA.¹⁷

3.1. The last step: the Regulation on the transparency and targeting of political advertising

The Digital Services Act is one of the most important innovations in recent years in defining a system of rules governing the digital services market and protecting EU users' rights.

However, the EU legislator, aware that an ad-hoc intervention was necessary to regulate specifically the use of online political and electoral propaganda, has recently approved a further regulation: we refer to the 'Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on transparency and targeting of political advertising'.

Except for a few limited provisions, it will apply from 2025 in all Member States (so that the last European elections of June 2024 were excluded).

The regulation aims, on the one hand, at contributing to the proper functioning of the internal market for political advertising and related services; on the other hand, at protecting natural persons regarding the processing of personal data.

The proposal moves along two main lines. First, it provides for a series of transparency and diligence obligations on 'political advertising service providers', defined as 'a natural or legal person engaged in the provision of political advertising services'. 'Political advertising', on the other hand, is defined as 'the preparation, placement, promotion, publication, delivery or dissemination, by whatever means, of a message normally provided in return for remuneration or through in-house activities or as part of a political advertising campaign: (a) by, for or on behalf of a political actor, unless of a purely private or purely commercial nature; or (b) which can and is intended to influence the outcome of an election or referendum, voting behavior or a legislative or regulatory process, at Union, national, regional or local level' (art 3).

The regulation requires, at art 11, that publishers of political advertising shall ensure that each political advertising message clearly, prominently and unambiguously displays the following information: (a) a statement attesting that it is a political advertising message; (b) the sponsor of the political advertising message and, where possible, the entity that ultimately controls the sponsor; (c) an indication of the election, referendum or legislative or regulatory process to which the political advertising message in question is related; (d) a statement attesting that the political advertising message has been the subject of targeting or message delivery techniques; (e) a transparency notice containing the

17 G Vigevani, 'Piattaforme digitali private, potere pubblico e libertà di espressione' (2023) 1 Diritto costituzionale 41, 41ff.

information required by the Regulation itself. In addition, publishers of political advertisements must allow natural or legal persons to report that a particular political advertisement published by them does not comply with the regulation and must set up a suitable notification system for this purpose. These requirements follow the warnings of the European Data Protection Supervisor and, precisely, are additional and supplementary to the transparency obligations, laid down in the Digital Services Act, abovementioned.

These obligations should make data controllers more accountable, since the keeping of specific registers and greater transparency on targeting techniques should encourage platforms to process user data in a way that complies with the law, and no longer evade existing obligations. Secondly, transparency rules should protect political actors, who should be more aware of how targeting works. However, the most significant advantage should be for citizens-users, who should be able to check the main parameters used to send them political ads: this should contrast targeting opacity and make users more aware of how electoral communication works in the digital era.

On the other hand, the regulation establishes that the processing of personal data is permitted due to certain conditions. Targeting or message delivery techniques in online political advertising are allowed if: a) the data controller has collected personal data from the data subject; (b) the data subject has given his or her explicit consent due to Regulations (EU) 2016/679 and (EU) 2018/1725 to the separate processing of personal data for political advertising purposes; (c) and such techniques do not involve ‘profiling’ as defined in Article 4(4) of Regulation (EU) 2016/679 and Article 3(5) of Regulation (EU) 2018/1725.

Compared to the prohibition in the first version of the proposal, which provided for several exceptions, the European Parliament and the Council have chosen, in the latest approved version, a stricter line, thus establishing an absolute prohibition of targeting for certain categories of data, considered particularly sensitive.

With reference to data that are not subject to special protection, processing is limited to that which is the result of the explicit consent of the data subject, given solely for the purposes of online political advertising. The regulation has a more restrictive wording than the original proposal, which did not provide for any additional limitation with respect to what was already prescribed by the GDPR. It is an important novelty since online platforms have to obtain express consent for processing from users. However, the European legislator seems to continue to ignore that the consent, given online by the user, is not informed, conscious and free, since the platforms’ policies are not clear and understandable.¹⁸

18 M Monti, ‘La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell’Unione Europea (Code of practice on disinformation)’ (2020) 11 *Federalismi* 282.

Finally, special protection is provided for minors, since targeting or advertising message delivery techniques involving the processing of personal data of a minor are prohibited.

In conclusion, the regulation recently approved by the European Parliament on March 2024 constitutes an important response to the critical issues repeatedly highlighted by both the European and national authorities as well as the doctrine: in particular, it is the first regulation specifically dedicated to the regulation of political advertising in pre-election periods.

However, some issues and doubts arise, and, in particular, a long process of implementation is necessary. For instance, the EDPS had suggested introducing a general and absolute ban on targeting for political purposes, since the obligations stated by the EU legislator might be insufficient in the face of the great variety of ways in which users can be profiled online, especially by using data that are not in considered 'sensitive', the so-called 'inferred data'.

In conclusion, the choice of the European legislator seems to be a reasonable compromise, considering the legitimate economic interests of Internet platforms, which base their business precisely on the processing of data for marketing purposes.¹⁹

4. Concluding remarks

Political targeting concerns several issues: from the need to preserve the individual citizen's right to free and informed information, to the need to protect economic interest of internet platforms, to, finally, the need to guarantee the prerequisites of political representation and participation, allowing genuine public debate inspired by deliberative principles.²⁰ All these issues are particularly important during electoral campaigns since targeting might influence the outcome of elections.

In a framework in which internet platforms are playing a key role, governing the online space, it was necessary to leave an approach based on self-regulation. This is what the European Union has put in place, recently approving several regulations.

They represent a first, significant, response, but not yet comprehensive and sufficient, as a long process of implementation of these new rules and of evaluation of the impact assessment is required.

More generally, the European strategy is shareable due to the trans-nationality of online political communication, even though some questions arise. On

19 See M Z van Drunen, N Helberger and R O Fathaigh, 'The beginning of EU political advertising law: unifying democratic visions through the internal market' (2022) 30(2) *International Journal of Law and Information Technology* 181.

20 See C Caruso, 'Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo' (2023) 3 *Quaderni costituzionali* 543.

the one hand, over-regulation could make the internal market safer, but also less competitive: online platforms could devise strategies to bypass the provisions set by the EU or, as a last resort, leave the European market, even though it is very profitable, boasting more than 250 million users; on the other hand, some areas have remained uncovered, exposing to the risk that these obligations could be circumvented by treating inferred data, i.e. data whose processing is not subject to special conditions and which are used to trace back to information for which processing is prohibited.

In conclusion, the new EU regulations have marked a decisive change in the European regulatory framework on profiling and targeting. It is now necessary to verify whether and how this new set of rules will be applied, with the aim of building an 'European digital space', which protects users' rights without threatening the freedom of economic initiative of Internet platforms, as well the freedom of propaganda of political parties, which use targeting for political purposes.

SECTION 3 – CRIMINAL MATTERS

Taking Defence Rights Seriously. The Need for Explainable Artificial Intelligence in Criminal Proceedings – A European Perspective

Marcia Michalina

University of Wrocław

ORCID 0000-0002-7872-8507

DOI: 10.54103/milanoup.215.c463

Abstract

The integration of artificial intelligence (AI) into criminal proceedings introduces both opportunities and challenges, also regarding the protection of defence rights. This article examines the intersection of AI, the right of defence and procedural fairness from a European perspective. It presents the hypothesis that the current deployment of AI in criminal justice systems presents more risks than benefits to defendants, particularly due to issues such as the black box problem and limited explainability of AI systems. The research explores how inadequate practice of AI systems implementation undermines key rights, including the right to information, defence preparation, legal assistance, translation and also equality of arms. The objectives include assessing whether the AI application can infringe defence rights and in what way, identifying the need for explainable AI (xAI), and proposing solutions to mitigate the risks posed by AI use in criminal trials. The methodology involves a review of European legal frameworks (regarding both defence rights standards and AI), case law, and practical examples of AI applications in criminal proceedings, supported by analysis of technical and human rights implications of AI systems like predictive analytics, natural language processing, and image recognition. Findings highlight critical gaps in regulation, emphasising the necessity for xAI to ensure transparency, effective participation, and trust in judicial processes. Recommendations include adopting a further harmonised legal framework for AI in criminal proceedings and implementing explainability measures tailored to defendants' needs.

Keywords

Artificial Intelligence, Right of Defence, xAI, Criminal Proceedings

1. Introduction

The technologically-based measures have deeply affected criminal proceedings in recent years. The need for digitalization was demonstrated by the COVID-19 spread and dissemination of remote court hearings.¹ Many controversies were also raised by surveillance technologies such as Pegasus, on-line searches and new lie-detecting technologies.² One of the most advanced technologies that is believed to significantly modify the course of proceedings is Artificial Intelligence (AI). Although the AI use has been mainly connected with and developed in the private law,³ recently the topic has gained significant interest from the public law perspective. The use of novel technology in the criminal proceedings, including some of the AI systems, appears to be inevitable, especially due to possible advantages of their implementation.

Application of AI systems comes with both risks and benefits. AI-based systems are believed to facilitate many activities taking place during the course of proceedings. They can make them more effective, efficient, quicker and eliminate bias rooted in the human factor.⁴ The most commonly describes risks are connected with bias and right to privacy, but they can also negatively influence

-
- 1 Krešimir Kamber, 'The Right to a Fair Online Hearing' (2022) 22 (1) Human Rights Law Review 1, 'The Practice Magazine' (*Harvard Law School Center on the Legal Profession*) <<https://clp.law.harvard.edu/knowledge-hub/magazine/>> accessed 20 March 2023, Ilze Tralmaka 'Defence Rights in Remote Justice Procedures' (*UN Office on Drugs and Crime*) <<https://www.unodc.org/dohadecclaration/en/news/2020/06/defence-rights-in-remote-justice-procedures.html>> accessed 30 May 2024.
 - 2 Orin S Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 Columbia Law Review 279, Michele Simonato, 'Defence rights and the use of information technology in criminal procedure' (2014) 85 *Revue internationale de droit pénal* 261, Sunil Bector, "'Your Laptop, Please.'" The Search and Seizure of Electronic Devices at the United States Border' (2009) 24 *Berkeley Technology Law Journal* 695, Bruce Luber and others, 'Non-Invasive Brain Stimulation in the Detection of Deception: Scientific Challenges and Ethical Consequences' (2009) 27 *Behavioral Sciences & the Law* 191.
 - 3 Commission, Directorate-General for Justice and Consumers, *Liability for Artificial Intelligence and Other Emerging Digital Technologies. Report from the Expert Group on Liability and New Technologies – New Technologies Formation* (Publications Office of the European Union 2019), Jochen Hanisch, *Haftung für Automation* (Cuvillier 2010), Michael Faure, Louis Visscher and Franziska Weber, 'Liability for Unknown Risks – A Law and Economics Perspective' (2016) 7 *Journal of European Tort Law* 198, Eric Hilgendor and Susanne Beck (eds) *Robotik und Gesetzgebung. Beiträge der Tagung vom 7. bis 9. Mai 2012 in Bielefeld* (Nomos 2013).
 - 4 Sray Agarwal and Shashin Mishra, 'Introduction' in Sray Agarwal and Shashin Mishra (eds), *Responsible AI: Implementing Ethical and Unbiased Algorithms* (Springer International Publishing 2021), Daniel Crevier, *AI: The Tumultuous History of the Search for Artificial Intelligence* (Basic Books 1993).

other human rights, including rights of defence, on which the article will focus.⁵ The main hypothesis of this article is that currently the use of systems based on the AI in criminal proceedings is more of a threat than a benefit to the right of defence.

Due to the use of AI systems and lack of sufficient regulation on explainable intelligence, right of defence could be significantly restricted, especially with regard to the right to information and the black box problem.⁶ Right to information, to prepare the defence and to an active participation in the proceedings is not effective when gathered evidence materials are incomprehensible and the decision-making process is unclear. The current state of regulation on the European Union (EU) level and in majority of Member States still does not sufficiently safeguard the right of defence and does not provide adequate means for review.⁷ This can lead to aggravating data bias and limiting the quality of individual rights. The use of defence-assisting systems is also underregulated. Although the black box problem has been addressed several times, some examples of explainable AI (xAI) have appeared,⁸ and even some attempts to regulate the issue have been made,⁹ the article argues that there are still many practical difficulties with an effective execution of procedural rights. Therefore, the need for regulation and safeguarding explainability, especially considering criminal proceedings specifics, is still valid.

The article focuses on the European perspective. More specific approach to the problem can lead to presenting more precise conclusions. It will allow to analyse the scope of defence rights applicable to the particular system and establishing the point of reference. Due to many differences among the particular regions in this regard (eg between US, EU, regional and universal ones), clarifying the chosen standard is crucial as it may result in recreating the coherent set of rights and adapting them to the new technological demands.

The first part of the article focuses on defining the AI and determining general applications and problems caused by the AI use in the defence rights context. The existing definitions on the AI and basic elements of the AI systems, such as machine learning and neural networks are briefly analysed. The article further introduces the concept of the black box problem and xAI – methods

5 Michele Caianiello, 'Criminal Process Faced with the Challenges of Scientific and Technological Development' (2019) 27 *European Journal of Crime, Criminal Law and Criminal Justice* 267.

6 For the definition see below – s 2.3.

7 Center for AI and Digital Policy, 'Artificial Intelligence and democratic values index' <<https://www.caidp.org/reports/aidv-2021/>> accessed 30 May 2024.

8 Stephen K Reed, 'Explainable AI' in Stephen K Reed (ed), *Cognitive Skills You Need for the 21st Century* (OUP 2020), Joanna J Bryson, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (OUP 2020).

9 eg in the AI Act and the Proposal for the AI Act (see further para 2.3).

of its achievement, scope and attempts to regulate the matter – as well as the practical risks connected with the black box, especially due to the proven track of bias of the AI systems. In this part the research is mainly based on the existing literature and analysis of legal acts, especially the Artificial Intelligence Act¹⁰, supported by the empirical research elements with regard to publicly available information on the systems used.

The next part covers the examples of AI systems and possibilities for their application in the criminal proceedings. It presents the general types of AI systems that are or can be used in criminal proceedings. Then the contribution explores, how they can affect the right of defence. The main basis for recreating the EU standard on the right of defence is the European Convention on Human Rights (ECHR)¹¹ and case law of the European Court of Human Rights (ECtHR). It creates a minimum European standard for all Council of Europe members, setting an optimum reference point for analysis also from the EU perspective.¹²

Finally, the article aims to propose possible solutions to the described problems, answer the main research question, if the current state of regulation safeguards the defence rights to the sufficient extent. Its objective is also to analyse if explainability is needed to safeguard effectiveness of defence rights and which ways to achieve xAI can be most beneficial to the defendant. Then the article seeks to answer if issuing legally binding act on the EU level is needed and what guarantees or requirements should be introduced by the legislator.

2. Artificial Intelligence and xAI

2.1 Defining AI and AI systems

Establishing one, common definition of the artificial intelligence has been one of the most problematic issues of the AI-focused literature and practice. Currently there exist many definitions of this term that very much differ. One

10 European Parliament, Legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA(2024)0138, hereinafter as the ‘AI Act’.

11 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

12 The ‘Explanations relating to the Charter of Fundamental Rights of the European Union’ [2007] (OJ C 326) on the arts 47 and 48 (right to an effective remedy and to a fair trial, presumption of innocence and right of defence) directly refer to the ECHR. Also, according to the art 6(3) of the Consolidated Version of the Treaty on European Union [2016] OJ C202/1, fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States are the element of the EU law principles.

of the major works on collecting the existing definitions of AI was made by the Joint Research Centre (JRC) of the European Commission which proposed an operational definition of AI formed by ‘a concise taxonomy and a set of keywords that characterize the core and transversal domains of AI’.¹³ These common characteristics would be consideration of the real world complexity, information processing, decision making, achievement of specific goals.¹⁴ Another definition in EU was proposed by the High Level Expert Group on Artificial Intelligence, which was much more complex and described AI systems as ‘software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions’.¹⁵

The existing definitions still raise many doubts as to their scope and content.¹⁶ There even have appeared statements that creating and adopting one common definition of AI is not needed at all and can be seen as restricting and unnecessary.¹⁷ The definitions that are being constructed in the upcoming regulations tend to approximate and focus on some common elements that constitute the AI in the general comprehension. The AI Act defines AI system as a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs

13 Sofia Samoilu and others, *AI Watch: Defining Artificial Intelligence: Towards an Operational Definition and Taxonomy of Artificial Intelligence* (Publications Office of the European Union 2020); Sofia Samoilu and others, *AI Watch, Defining Artificial Intelligence 2.0: Towards an Operational Definition and Taxonomy for the AI Landscape* (Publications Office of the European Union 2021).

14 Gianluca Misuraca and Colin Van Noordt, *AI Watch - Artificial Intelligence in Public Services* (Publications Office of the European Union 2020).

15 Independent High Level Expert Group on AI (AI HLEG), ‘A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines | Shaping Europe’s Digital Future’ (8 April 2019) <<https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>>. It also specified that as a scientific discipline, AI includes ‘several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)’.

16 Joanna J Bryson, ‘Europe Is in Danger of Using the Wrong Definition of AI’ *Wired* <<https://www.wired.com/story/artificial-intelligence-regulation-european-union/>> accessed 4 April 2023.

17 Manuel A Utset, ‘Predictive Policing and Criminal Law’, in John McDaniel and Ken Pease (eds), *Predictive Policing and Artificial Intelligence* (Routledge 2021).

such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law¹⁸ adopts a very similar definition and describes AI system as a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. The Conventions states that different AI systems vary in their levels of autonomy and adaptiveness after deployment.

It became clear that there are some basic AI-specific elements that differentiate it from other common algorithms and represent its basic core.¹⁹ It is, first of all, the ability to learn, reason and make decisions. The aim of the reasoning, to put it simply, is to present solutions of the defined problems without the human intervention. It is an essential part of the knowledge representation and reasoning part of the AI. The decision-making part is an element of the process that allows to obtain a final result and reach the aim of the AI systems use. The part mostly differentiating AI systems from ordinary algorithm-based ones is an ability to learn. To simplify, the self-learning program should, on the basis of the input data entered into the system and in connection with the expected output, modify and shape the rules for processing data itself, and thus learn through its experience. Several types of machine learning can be distinguished that demand various degrees of human impact.

Supervised learning allows to determine the relationship of specific inputs to outputs based on labelled examples of pairs of both types of data provided to the system. The implemented patterns can then provide examples for future use, based on the similarity of the situation, environment, etc. Supervised learning most often requires a significant amount of data and human action, especially data labelling.²⁰ Unsupervised learning features a greater degree of autonomy in the AI systems. The input data is not subject to prior labelling, and the system itself aims to find patterns in the datasets. The AI-based system is supposed to find the links that exist between the data, which should be identified with increasing accuracy as the system continues to operate. As a result it should achieve the goals set for the AI use. Systems in this case can function

18 Committee of Ministers of the Council of Europe (133th Session), ‘Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law’ (17 May 2024 Strasbourg), that will be opened for signature on the occasion of the Conference of Ministers of Justice in Vilnius on 5 September 2024.

19 This approach is the most similar to the definition provided in Sofia Samoilis and others, *AI Watch* (n 13) and Sofia Samoilis and others, *AI Watch 2.0*. (n 13).

20 Pádraig Cunningham, Matthieu Cord and Sarah Jane Delany, ‘Supervised Learning’ in Matthieu Cord and Pádraig Cunningham (eds), *Machine Learning Techniques for Multimedia: Case Studies on Organization and Retrieval* (Springer 2008).

more independently and rely less on human intervention.²¹ The semi-supervised learning combines elements of the two types of machine learning mentioned above - both labelled and unlabelled input data are introduced to the system.²²

There can be also distinguished other specific types of machine learning, for example reinforcement learning, which relies on the system's search for solutions and ways of data processing to maximize the result in a given environment. The system provides for the environment analysis, most often subject to many variables, and by learning through its experience aims to achieve the desired effect.²³ Finally, there is deep learning, that does not necessarily constitute different mode of machine learning, but is strictly related to the type of system and its basis on which machine learning is based in this case - artificial neural networks.

2.2 Artificial neural networks

The basis of many modern artificial intelligence-based systems and deep learning algorithms are formed by neural networks, also referred to as artificial neural networks (ANNs).²⁴ The term neural network refers to the way the human brain functions.²⁵ The basic unit in this case is the so-called node, an artificial neuron, which is provided with an input, an output and a dataset storing weights.²⁶ Each of these nodes connects to the others, collects the input signals, recalculates them and sends the output signal to the next layer. The artificial neuron has a specific associated weight and threshold (connection - hence connectionist AI). If the output data exceeds the assigned threshold value, the specified node will be activated and the data will be sent to the next layer of the network.²⁷

-
- 21 Salim Dridi, 'Unsupervised Learning - A Systematic Literature Review' (13 June 2024) OSF Preprints <<https://osf.io/preprints/osf/mpkht>> accessed 30 May 2024.
 - 22 Jesper E van Engelen and Holger H Hoos, 'A Survey on Semi-Supervised Learning' (2020) 109 Machine Learning 373, Y Reddy, Viswanath Pulabaigari and Eswara B, 'Semi-Supervised Learning: A Brief Review' (2018) 7 International Journal of Engineering & Technology 81.
 - 23 Wolfgang Ertel, 'Reinforcement Learning' in Wolfgang Ertel (ed), *Introduction to Artificial Intelligence* (Springer International Publishing 2017).
 - 24 Akash Goel, Amit Kumar Goel and Adesh Kumar, 'The Role of Artificial Neural Network and Machine Learning in Utilizing Spatial Information' [2022] Spatial Information Research <<https://doi.org/10.1007/s41324-022-00494-x>> accessed 30 May 2024.
 - 25 Ralph Adolphs, 'Cognitive Neuroscience of Human Social Behaviour' (2003) 4 Nature Reviews Neuroscience 165.
 - 26 N Jindal and V Kumar, 'Enhanced Face Recognition Algorithm Using PCA with Artificial Neural Networks' (2013) <<https://www.semanticscholar.org/paper/Enhanced-Face-Recognition-Algorithm-using-PCA-with-Jindal-Kumar/d7244f2ab95483b68b97a346e40eb-f6ad919e1e7>> accessed 29 April 2023.
 - 27 'AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?' (IBM 6 July 2023) <https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks> accessed 30 May 2024.

The functioning of neural networks is based on the layers within which the neurons are arranged. The outer layer registers data inputs from outside and processes them. It then passes this information to the next layer, which is already referred to as a hidden layer. The hidden layer recalculates and processes the acquired information and then also passes the information to the next hidden layer or output layer. The output layer processes the aggregated data and information from the previous layers, makes the final calculations and sends the result to the user, which takes the form of making a specific decision.²⁸

The use of neural networks allows for higher efficiency of the AI systems and processing huge amounts of information. Combined with machine learning, especially deep learning, constitutes the biggest advantages of the AI and can result in spectacular effects, exceeding human possibilities. However, it also causes some fundamental problems in the AI ethics domain.

2.3 Explainable AI

One of the main issues connected with the use of AI is the black box problem. Its essence comes down to the inability to thoroughly track how an AI-based mechanism produced a given result and tracing its inner processing.²⁹ The black box is in fact mainly associated with machine learning, especially unsupervised and neural networks based systems. In the case of complex mechanisms based on machine learning, input data and output datasets are fed into the algorithm, which, in combination, are supposed to lead the algorithm to develop optimal methods for achieving its designated goals. This process, however, is not based on explicit, clear rules, adapted to the typical ways and capabilities of human reasoning.³⁰ The hidden layers of nodes process input data and pass partial output data onto the next layer. The way the systems function does not allow for the results of the processes between the layers to be fully tracked. It is only possible to observe the final output data, which does not allow to learn how the system itself works and how it makes decisions.³¹ So, we have a self-learning algorithm that issues recommendations, makes analysis or

28 Richard E Neapolitan and Xia Jiang, *Artificial Intelligence: With an Introduction to Machine Learning, Second Edition* (2nd edn, Chapman and Hall/CRC 2018).

29 Carlos Zednik, 'Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence' (2021) 34 *Philosophy & Technology* 265.

30 Gabriëlle Ras, Marcel van Gerven and Pim Haselager, 'Explanation Methods in Deep Learning: Users, Values, Concerns and Challenges' in Hugo Jair Escalante and others (eds), *Explainable and Interpretable Models in Computer Vision and Machine Learning* (Springer International Publishing 2018).

31 Michael Pfeiffer and Thomas Pfeil, 'Deep Learning With Spiking Neurons: Opportunities and Challenges' (2018) 12 *Frontiers in Neuroscience* <<https://www.frontiersin.org/articles/10.3389/fnins.2018.00774>> accessed 28 March 2023; Vanessa Buhrmester, David Münch and Michael Arens, 'Analysis of Explainers of Black Box Deep Neural Networks for Computer Vision: A Survey' (2021) 3 *Machine Learning and Knowledge Extraction* 966.

predictions that serve as a basis for the final decision of a competent authorities in criminal proceedings that can be unexplainable. As a result, it can cause some serious problems within the right of defence.

There has been a long debate over the issue of explainability and different approaches to this problem have been distinguished. For example, explainability can be supported by providing the broad information about the system used which is not decision or input-data specific (so called global interpretability). This information can include setup information, training metadata, performance metrics, process information.³² Such explainability can guarantee the proper quality control, especially over the input data and allow defendant to check for eg implemented anti-bias procedures.

The local interpretability (subject – centric as it mainly concentrates on the subject of the decision or recommendation) models can provide information about the characteristics of individuals who received similar decisions.³³ The interpretations are based on the input data and do not give the explanations about the model as a whole, but narrow it down to the chosen variables.³⁴ For example, the convicted person could receive real information on what elements influenced the penalty imposed.

The decompositional approach on the other hand attempts to explain inner workings or replicate reasoning of the system. One of the most common methods is creating the surrogate model, that does not have access to the inner workings of the primary AI model and internal weights of the model, but works by analysing featured input and output data pairs. A model is constructed based on modelling the response of the simulator to a limited number of intelligently chosen data points.³⁵ In this case defendant would presumably be able to learn about how the system came to its conclusions.

32 Ashley Deeks, 'The Judicial Demand for Explainable Artificial Intelligence' (2019) 119 *Columbia Law Review* 1835, Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (23 May 2017) [2017] *Duke Law & Technology Review* 18–84.

33 Edwards and Veale (n 32) 57–59, Danielle Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1, 28–29.

34 Edwards and Veale (n 32) 59.

35 W Andrew Pruett and Robert L Hester, 'The Creation of Surrogate Models for Fast Estimation of Complex Model Outcomes' (2016) 11 *PLoS ONE* e0156574, Deeks (n 32) 1838.

The explainability issues have been raised in almost every recommendation of international bodies, including Council of Europe³⁶, OECD³⁷, and UN³⁸. In the most recent years such recommendations have been transferred into regulatory proposals. Transparency obligations have been introduced to the Council of Europe Convention on AI and reflected in the UN General Assembly Resolution³⁹. More explicit and specific attempts to introduce some explainability-oriented solutions can be found in the AI Act. The Regulation contains provisions relating to the input data quality control and guidelines on designing and developing the systems, maximizing the traceability. High-risk AI⁴⁰ systems should enable the automatic recording of events ('logs') while the systems is operating throughout its lifecycle. Moreover, the AI systems provider should ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. Chapter 3 of the AI Act obliges, *inter alia*, to draw up technical documentation, conformity assessment and quality management system.

Finally, the high-risk AI systems should guarantee the possibility for human oversight and that they can be effectively overseen by natural persons during the period in which the AI system is in use. Human oversight is one of the postulates frequently appearing in the recommendations addressing the AI ethics domain.⁴¹ This oversight, according to the AI Act, should aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose.

The Proposal for the AI Act⁴² introduced obligations that the provider was expected to fulfil for the benefit of the user. It defined 'user' as 'any natural or

36 Council of the European Union, 'Shaping Europe's Digital Future' (Conclusions, 9 June 2020), *idem*, 'Artificial intelligence: Presidency issues conclusions on ensuring respect for fundamental rights' (Oct. 21, 2020), *idem*, 'The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change' 11481/20 (Presidency Conclusions, 21 October 2020).

37 Global Privacy Assembly, 'Adopted Resolution on Accountability in the Development and Use of Artificial Intelligence' (October 2020) <<https://globalprivacyassembly.org/wp-content/uploads/2020/11/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf>> accessed 30 May 2024.

38 UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (2021), UNSG 'Roadmap for Digital Cooperation' (June 2020).

39 UNGA, Res 78/L.49 (13 March 2024) UN Doc A/78/L.49.

40 See in particular the Annex III to the Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts', COM (2021) 206 final (hereinafter also as 'Proposal for the AI Act').

41 Council of Europe, Committee of Ministers, *Ad hoc* Committee on Artificial Intelligence (CAHAI), 'Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law' CM(2021)173-add (17 December 2021).

42 See Proposal for the AI Act.

legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity' (art 3(4)). According to this definition, the court or the law enforcement agencies could be perceived as users. However, when the State (the court, prosecutor etc.) would introduce the results of AI systems into the proceedings, there were still no sufficient safeguards for the person affected by the use of such systems – the defendant.

In the final text of the AI Act, due to the amendments proposed by the European Parliament, the position of the defendant in the light of the explainability requirements, shifted and improved to some extent. The AI Act introduces a definition of the 'deployer' as a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. This allows the term to cover both State and private entities that implement the AI systems directly into their activities. In the amendments of the European Parliament, there also appeared a term 'affected person' defined as 'any natural person or group of persons who are subject to or otherwise affected by an AI system'. The EU legislator clearly saw the need to differentiate and regulate the situation of these two groups of entities.

According to art 13 of the AI Act, high-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately. Types and degrees of transparency should correspond with the relevant obligations of the provider and deployer set out in Section 3 of the Act. The article also imposes an obligation to provide the deployers with a detailed information on the AI systems. This allows for making the primary step towards the explainability - it is first of all necessary for the deployers to understand and interpret the AI system to give any real information to the person affected by its use.

The AI Act introduces also the next step – the right to explanation of individual decision-making. According to art 86, as a rule, any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights should have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

The AI Act introduces, therefore, an enforceable right directly attributable to a person affected by the algorithm, potentially also a defendant. It creates a step towards at least a local explainability. Based on this provision defendants should possess a real ability to gain insight into the decision taken and main parameters of the AI system involvement. This provision, however, can be subjected to exceptions (art 86(2)) and has not necessarily been adjusted to the

criminal proceedings specifics. The final wording of the AI Act also deprived the affected person the explicit insight into the input data. Also, without the national transposition, the awareness of such rights can be in fact minimal. Finally, the provision does not constitute a solution to all problems connected to lack of real explainability of AI systems and information about the reasoning of the system.

3. AI in criminal proceedings

3.1 Examples of the systems used in criminal proceedings

The AI systems, in particular in pre-trial stage, can be used for the purpose of individual and general prevention and policing.⁴³ Data obtained through the use of AI could be also applied as evidence that would be gathered by the law enforcement agencies and used in the further course of the proceedings.⁴⁴ When it comes to issues connected primarily with the judicial stage of the proceedings, the biggest controversy is, of course, the possibility of decision-making by intelligent agents.⁴⁵ However, much more likely and common than the vision of judge-robot's independent judgments are systems that assist in reaching a certain type of decision. They can also signal possible omissions, mistakes or propose and calculate, for example, the elements of the punishment assessment based on the data entered by the judge.⁴⁶ High hopes for streamlining the course of the criminal proceedings also associated with speech recognition systems and the translation of evidence using AI.⁴⁷ AI systems use can be used in different dimensions, including natural language processing (NLP), image recognition and predictive analysis. Although they often intersect, each of them

43 See eg Stefanie Hännold, 'Profiling and Automated Decision-Making: Legal Implications and Shortcomings' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgo (eds), *Robotics, AI and the Future of Law* (Springer Singapore 2018) 123–153.

44 Sabine Gless, 'AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials' (15 May 2020) <<https://papers.ssrn.com/abstract=3602038>> accessed 28 March 2023.

45 Tony Ho Tran, 'China Created an AI "Prosecutor" That Can Charge People with Crimes' (*Futurism*) <<https://futurism.com/the-byte/china-ai-prosecutor-crimes>> accessed 28 March 2023.

46 Aleš Završnik, 'Criminal Justice, Artificial Intelligence Systems, and Human Rights' (2020) 20 ERA Forum 567–583.

47 Blessing Oyetunde, 'Introducing Salme, Estonian courts' speech recognition assistant', (*e-Estonia*, 26 January 2022) <<https://investinestonia.com/introducing-salme-estonian-courts-speech-recognition-assistant/>> accessed 28 March 2023, European Union Agency for Fundamental Rights (FRA), 'Artificial Intelligence, Big Data and Fundamental Rights Country Research Estonia, 2020', <https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-estonia-country-research_en.pdf> accessed 28 March 2023.

can find different application and have their own specifics affecting the needs of the parties to the proceedings.

3.1.1 Natural language processing

Natural language processing (hereinafter: NLP) combines computational linguistics with statistical models, machine learning, including deep learning. It enables computational mechanisms to process human language in the form of text or sound and ‘understand’ its meaning, including even the intentions and feelings of the author of the text, or the person delivering it.⁴⁸ Programmes using NLP perform tasks such as detecting and segmenting speech or text, tagging parts of it, encoding meanings, delivering references, and generating text themselves.⁴⁹

NLP techniques are used in various types of data analysis tools, to detect and dispose of redundant information, to create virtual assistants or chat bots, and to abbreviate, analyse text and perform machine translation. AI systems using NLP are able to process huge amounts of data in a very short time, handle a significant number of grammatical rules specific to different languages, and perform simultaneous translation. NLP programmes are also used for information gathering, search and retrieval, evidence processing and analysis, as well as for question-answering software.⁵⁰

They also offer extensive opportunities in the legal field. It is on natural language processing, especially in the form of Large Language Models (LLMs), that assisting chatbots are based, such as ChatGPT,⁵¹ Automio,⁵² BillyBot,⁵³ tools that search for information and answer legal questions through vast resources of databases, such as Ross,⁵⁴ DoNotPay,⁵⁵ assisting in challenging fines, addressing small claims or discrimination cases, and the LISA Robot Lawyer,⁵⁶ among others. NLP can assist both individuals without legal knowledge and professional lawyers who can use these tools to reduce the time spent on

48 Irene Solaiman and Christy Dennison, ‘Process for Adapting Language Models to Society (PALMS) with Values-Targeted Datasets’ (*arXiv*, 23 November 2021) <<http://arxiv.org/abs/2106.10328>> accessed 20 April 2023.

49 Brojo Kishore Mishra and Raghvendra Kumar (eds), *Natural Language Processing in Artificial Intelligence* (Apple Academic Press 2020).

50 Ivano Lauriola, Alberto Lavelli and Fabio Aiolli, ‘An Introduction to Deep Learning in Natural Language Processing: Models, Techniques, and Tools’ (2022) 470 *Neurocomputing* 443–456, Pascal Muam Mah, Iwona Skalna and John Muzam, ‘Natural Language Processing and Artificial Intelligence for Enterprise Management in the Era of Industry 4.0’ (2022) 12 *Applied Sciences* 9207.

51 <<https://openai.com/blog/chatgpt>> accessed 28 March 2023.

52 <<https://firmsy.com/>> accessed 28 March 2023.

53 <<http://www.billybot.co.uk/>> accessed 28 March 2023.

54 <<https://blog.rossintelligence.com>> accessed 28 March 2023.

55 <<https://donotpay.com/>> accessed 28 March 2023.

56 <<https://robotlawyerlisa.com/>> accessed 28 March 2023.

simpler tasks. They can be used both for the purposes of civil and criminal proceedings. Finally, these programmes will also assist law enforcement and the judiciary themselves not only as assistive tools for search activities, but also for the translation of documents in proceedings.

3.1.2 *Image recognition*

Another significant area of AI use is computer vision and image recognition. These terms are sometimes used interchangeably, but image recognition encompasses a range of techniques and processing activities, such as image identification, or image classification based on computer vision.⁵⁷

One of the measures used for crime detection and prevention is face analysis and face recognition. An AI algorithm can simultaneously not only detect and recognise a face, but also assess its layout, position, determine gender, age, emotions and so on. Face analysis based on ANNs, machine learning and computer vision allows image and video footage to be analysed to verify identity, background, health and even possible intentions. The systems can accurately recognise a face even if it has undergone some kind of transformation for example due to the ageing process. These systems may in part be intended for commercial use, but they can also be used for crime prevention and detection in law enforcement and evidentiary purposes.⁵⁸

AI systems will not be limited to face analysis alone - they can also include the analysis of objects, objects, shapes, patterns, etc. contained in photographs or video footage. These systems can also be used for security maintenance, detection of dangerous objects, such as in the case of security tools used at airports.⁵⁹ The image recognition and other computer vision tools can be also successfully applied for the purposes of evidence processing.

3.1.3 *Predictive analysis*

The overall aim of AI predictive analytics is to try to predict future outcomes based on pre-collected data and statistical modelling, data mining and machine learning. This analysis will rely on significant data resources (big data), for its practical use. In order to make any predictive estimates, the AI system will first need to process a range of information collected in various types of databases.

57 Poonam Yadav, Hukum Singh and Kavita Khanna, 'Computer Vision, Its Applications, and Challenges' (22 February 2022) Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022 available at <<https://papers.ssrn.com/abstract=4041050>> accessed 20 April 2023.

58 Antonio J Colmenarez and Thomas S Huang, 'Face Detection and Recognition' in Harry Wechsler and others (eds), *Face Recognition: From Theory to Applications* (Springer 1998).

59 Guadenz Boesch, 'Image Recognition: The Basics and Use Cases (2023 Guide)' (*viso.ai*, 10 December 2023) <<https://viso.ai/computer-vision/image-recognition/>> accessed 30 May 2024.

Then it needs to identify recurring patterns, relationships, or trends, and derive specific conclusions from this processing.⁶⁰ Predictive AI will be applicable both for use by lawyers – eg to try to predict the outcome of a case based on historically collected data, but it will also be an essential tool for authorities, especially the police and activities aimed at individual and general prevention and detection of crime.⁶¹

Some of the solutions have already been put into practice. Such systems have been implemented to predict the type of crime, its date, time and place of its commission. Examples in this regard include Risk Terrain Modeling,⁶² PredPol,⁶³ Italian X-Law,⁶⁴ KeyCrime,⁶⁵ German Precobs also used in Switzerland,⁶⁶ or British HART.⁶⁷ These systems can be used for general prevention, focusing on location-based tools, but can also be used to detect perpetrators of previously committed crimes.⁶⁸ In the case of investigative activities and real-time responses, ie taken in the time frame between deciding to commit a crime and committing it, they can also influence the final implementation of intent.⁶⁹ Individual-oriented systems such as COMPAS for example, have also come into use.⁷⁰ Systems that support the work of law enforcement agencies, such as facial recognition systems, DNA analysis, gunshot detection are also emerging with the use of artificial intelligence.⁷¹

60 Maciej Wach and Iwona Chomiak-Orsa, 'The Application of Predictive Analysis in Decision-Making Processes on the Example of Mining Company's Investment Projects' (2021) 192 *Procedia Computer Science* 5058.

61 Serena Quattrocchio, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, vol 4 (Springer International Publishing 2020) 39–40.

62 <<https://www.riskterrainmodeling.com/>> accessed 28 March 2023.

63 <<https://www.predpol.com/>> accessed 28 March 2023.

64 <https://www.xlaw.it/presentazione/index_eng.asp> accessed 28 March 2023.

65 <<https://keycrime.com/>> accessed 28 March 2023.

66 <https://www.stadt-zuerich.ch/portal/de/index/politik_u_recht/stadtrat/weitere-politik-felder/smartcity/english/projects/precobs.html>, <<https://land-der-ideen.de/en/project/precobs-software-for-predicting-crimes-355>> accessed 28 March 2023.

67 Marion Oswald and others, 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality' (2018) 27 *Information & Communications Technology Law* 223–250.

68 Quattrocchio (n 61) 39–40, Manuel A Utset (n 17), 163–183.

69 Utset (n 17) 173.

70 Danielle Kehl, Priscilla Guo and Samuel Kessler, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing' (*Berkman Klein Center for Internet & Society, Harvard Law School*, 25 August 2017) <https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf> accessed 22 March 2023.

71 Nipuni A Wickramaratna and Eata Edirisuriya, 'Artificial Intelligence in the Criminal Justice System: A Literature Review and a Survey' (*General Sir John Kotelawala Defence University*, 2022) <<http://ir.kdu.ac.lk/handle/345/5244>> accessed 30 May 2024, 4–5.

3.2 Risk of bias and malfunction

The examples given above are only a short summary of the possibilities of AI application within the criminal proceedings. The scope of tools available for use by both State actors and private entities, including lawyers and parties to the proceedings, is far wider. However, one of the major concerns that make this theoretical argumentation valid in a practical dimension is the fact, that the AI systems have the proven track record of bias. The most concerns have been raised in relation to racial discrimination⁷², but there are other issues connected eg with gender, sexual orientation or even disabilities.⁷³ The face recognition systems (including Microsoft, IBM, Megvii) have been proven of less accuracy in case of women and other ethnicities and races than Caucasian.⁷⁴ The systems can therefore appear imprecise and affect the final result of the proceedings, causing serious consequences for the people affected.⁷⁵ The natural language processing systems used eg in the translation and search-oriented tools, also reflect the bias and can contribute to perpetuation of the stereotypes.

Many controversies are connected with profiling systems. They have reflected racial, socioeconomical and gender bias. In case of gender, there can appear

72 Zo Ahmed, Bertie Vidgen and Scott A Hale, 'Tackling Racial Bias in Automated Online Hate Detection: Towards Fair and Accurate Detection of Hateful Users with Geometric Deep Learning' (2022) 11 EPJ Data Science 1, Will Douglas Heaven 'Predictive Policing Algorithms Are Racist. They Need to Be Dismantled' (*MIT Technology Review* 17 July 2020) <<https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/>> accessed 28 March 2023, 'Test Algorithms for Bias to Avoid Discrimination' (*European Union Agency for Fundamental Rights*, 30 November 2022) <<http://fra.europa.eu/en/news/2022/test-algorithms-bias-avoid-discrimination>> accessed 28 March 2023.

73 Lydia X Z Brown and others 'Ableism And Disability Discrimination In New Surveillance Technologies: How New Surveillance Technologies in Education, Policing, Health Care, and the Workplace Disproportionately Harm Disabled People' (*Center for Democracy and Technology*, 24 May 2022) <<https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/>> accessed 28 March 2023, European Network of National Human Rights Institutions (ENNHRI), 'Artificial Intelligence and Gender Equality: How Can We Make AI a Force for Inclusion, Instead of Division?' (ENNHRI, 8 March 2023) <<https://ennhri.org/news-and-blog/artificial-intelligence-and-gender-equality-how-can-we-make-ai-a-force-for-inclusion-instead-of-division/>> accessed 28 March 2023, Fabian Lütz, 'Gender Equality and Artificial Intelligence in Europe. Addressing Direct and Indirect Impacts of Algorithms on Gender-Based Discrimination' (2022) 23 ERA Forum 33.

74 The example can be a New Zealand case in which an Asian person was denied a passport due to 'closed eyes'. Can Yavuz, 'Machine Bias Artificial Intelligence and Discrimination' (Master thesis, University of Lund 2019), 'The Perpetual Line-Up' (*Perpetual Line Up*) <<https://www.perpetuallineup.org/>> accessed 28 March 2023.

75 Clare Garvie, Jonathan Frankle and Alvaro Bedoya 'Unregulated Police Face Recognition in America - Perpetual Line Up' (*George Town Law Center on Privacy & Technology*, 18 October 2016) <<https://www.perpetuallineup.org/>> accessed 28 March 2023.

the problem of so-called reverse discrimination, as the existing statistics are mainly focused on men.⁷⁶ There have been cases, where profiling overly targeted transgender or disabled people,⁷⁷ but mostly there have been severe cases of racial bias. The systems, such as COMPAS and other programs dedicated for individual prevention were introduced eg in Los Angeles and Chicago. Chicago launched a program, which relied on data from arrest records and social media to assess risk of participating in shootings. The result of this program was so-called “Strategic Subject List” that was meant to facilitate the work for the police. Due to controversies, the Programme was officially closed in 2020.⁷⁸

Generally speaking, the source of the problem is that machine learning models reflect the biases of those designing the systems, implementing them, and collecting certain data. The human influence cannot be separated from the collected data. This human factor can, especially in the light of the process of data training, influence the final decision making. Finally, even if there is no bias in the collected data, the system can simply produce an error.⁷⁹ As a result, it is necessary, that the court, but also the defendant and his lawyer can obtain the information on how the decision was made by the AI systems and why such recommendation was proposed.

3.3 Impact on defence rights

With such a broad scope of actions, AI systems can significantly impact the course of proceedings and influence decisions of the prosecutor and the court. However, with the explainability issues in mind and due to general complexity of the systems, the particular defence rights can appear ineffective. The use of new technologies in the criminal proceedings already raises serious controversies about the equality of the parties, especially in terms of surveillance.⁸⁰ The State in this case has many more measures, resources and information at its disposal. This disparity and doubts as to the effectiveness of particular rights are further deepened in the case of the implementation of AI systems into the proceedings.

ECHR in its art 6 divides general right of defence into particular rights. This division can be helpful to identify particular threats to the specific elements of

76 It can affect mostly other legal issues, connected with especially family law and granting the custody. Can Yavuz, ‘Machine Bias Artificial Intelligence and Discrimination’ (2019) <<https://www.researchgate.net/publication/334721591>> accessed 28 March 2023.

77 Lidia X Z Brown and others (n 73).

78 However, there still appear concerns that the Police uses it unofficially ‘Stop and Frisk | ACLU of Illinois’ (11 August 2017) <<https://www.aclu-il.org/en/campaigns/stop-and-frisk>> accessed 5 April 2023.

79 Sasanka Sekhar Chanda and Debarag Narayan Banerjee, ‘Omission and Commission Errors Underlying AI Failures’ [2022] AI & SOCIETY.

80 Radina Stoykova, ‘Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence’ (2021) 42 Computer Law & Security Review 105575.

defence rights. art 6(3) of the ECHR sets the minimum standard and the core of defence rights. It can be considered an optimum starting point for the analysis. The elements included in the article are:

- ‘(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
- (b) to have adequate time and facilities for the preparation of his defence;
- (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
- (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
- (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.’

Controversies with the AI use are mostly connected with the right to information and access to case files. The right to information is one of the basic rights of the defendant, which enables them to take action - both in response to the actions of the prosecution and on his own initiative. It provides means to ensure the active and effective participation of defence counsel in the proceedings as well. The right to information, broadly defined, encompasses not only the right to be informed about the nature and cause of the accusation and information about the charges, but also the right to be informed about the rights of the defendant.⁸¹ Knowledge of procedural rights is an essential safeguard of the effective use of defence rights in the course of the trial, while preventing possible abuse of power by the law enforcement agencies. It thus facilitates the implementation of the principle of equality of arms and the adversarial model of the trial.⁸²

The most important conclusion that can be drawn from ECtHR case law is that information must be clear, interpretable. The same may be applied to the case materials. According to ECtHR, the defendant should be able to draw clear conclusions from the case files, allowing them to conduct effective defence.⁸³ It should not be presented only as a formal fulfilment of an obligation, but should equip the defendant with the real tools to take action in the proceedings. Both information about the charges, their basis and evidence for their support should

81 European Court of Human Rights, ‘Guide on Article 6 of the Convention – Right to a fair trial (criminal limb)’ (29 February 2024), 34–35, 80–81.

82 *Pelissier and Sassi v France*, App no 25444/94 (ECtHR, 25 March 1999), para 54; *Dallos v Hungary*, App no 29082/95 (ECtHR 1 March 2001), para 47.

83 *Migoni v Poland*, App no 24244/94 (ECtHR, 25 June 2002); *Schops v Germany*, App no 25116/94 (ECtHR 13 February 2001); *Garcia Alva v Germany*, App no 23541/94 (ECtHR, 13 February 2001); *Lietzow v Germany*, App no 24479/94 (ECtHR, 13 February 2001).

be presented in such a way, that defendant can draw some useful conclusions for their case as such information will be useful to benefit from other rights enlisted in the art 6 ECHR.⁸⁴ So, if the defendant will be presented with the files but could not encode from them any real information, both the right to information and the right to have adequate time and facilities for the preparation of his defence will be put into question.

In case of defence in person, the defendant should be provided with an opportunity to effectively participate in the proceedings, and thus be equipped with a number of procedural rights that will guarantee them this effective participation. In addition to the already mentioned rights to information and access to case materials, the defendant also has the right to question the legitimacy of the procedural actions carried out, to present evidence in support of their claims, to file motions, submit evidence, and to question the decisions made during the proceedings.⁸⁵

The defence counsel, just like the defendant, must be given the actual opportunity to take action in the proceedings. The mere formal granting of the right to legal assistance is not a sufficient solution in the light of the current standards of the right to access to lawyer. The right of access to defence counsel should not be illusory requirement with no practical use, but existing regulations should, once again, guarantee the real effectiveness of this right. In order to be able to actually fulfil their role, the lawyer must have certain procedural measures at their disposal to ensure that they can actively participate especially in the evidentiary proceedings and exercise control over the course of the trial.⁸⁶ The aim and essence of the access to the lawyer is the ability to actively represent the defendant by first learning the facts, then establishing a line of defence

84 Stefan Trechsel, 'The Right to Be Informed of the Accusation' in Stefan Trechsel and Sarah Summers (eds), *Human Rights in Criminal Proceedings* (OUP 2006).

85 Stefan Trechsel, 'The Right to Defend Oneself and to Have the Assistance of Counsel' in Stefan Trechsel and Sarah Summers (eds) (n 84), Arkadiusz Lach *Rzeczelne postępowanie dowodowe w sprawach karnych w świetle orzecznictwa strasburskiego*, (Wolters Kluwer 2018) 125. *Lüdi v Switzerland* App no 12433/86 (ECtHR, 15 June 1992), paras 49-50; *Lucà v Italy* App no 33354/96 (ECtHR, 27 February 2001), para 39; *AAl-Khawaja and Tahery v UK* App no 2676/05 and 22228/06 (ECtHR, 15 December 2011), para 118.

86 Thomas Barkhuysen and others, 'Right to a Fair Trial', in Pieter van Dijk and others (eds) *Theory and practice of the European Convention on Human Rights* (Cambridge 2018) 637.

in consultation, confidentially (what is another crucial condition of the effective defence),⁸⁷ with the client, and finally conducting the defence at trial.⁸⁸

Consequently, if the defendant cannot draw any conclusions from the case materials or if they will be burdened by the flood of incomprehensible information, they will not be able to take any real actions and challenge it effectively. The same effect can appear with the defence counsel participation. In case of a significant digitalization, lack of transparency in the use of particular systems, the result can be the same as if the defence counsel did not take part in the proceedings at all. If there is no knowledge on the systems used and its working cannot be traced, the lawyer cannot in fact initiate any type of review and execute effective control over the course of the trial. When tracking the algorithm of AI either demands the specialist knowledge, not accessible to the average citizen, or is even impossible, the purposes of the right to information cannot really be met. As a result, the defendant in fact cannot effectively challenge the procedural actions on which his potential conviction could be based. Moreover, it is highly possible that the judge in most cases will also not possess the broad technological knowledge. Therefore the ability to assess the eventual malfunction, bias in the system or the disproportionality of the measure and in this regard refer to the appeal also should be put into question.⁸⁹

Similar problem arises with the right of translation. The right to translation has a significant impact on all defence rights. It is difficult to assume that the defendant can consciously and fully exercise his information rights or the opportunity to actively participate in the proceedings if they does not understand the content of proper instructions, charges or evidence gathered during the proceedings. It is crucial to the fairness of the proceedings and the effectiveness of the right of defence that the translation is of an adequate quality. The competent authorities (the court or the prosecutor) should watch over this quality, also through *ex post* reviews.⁹⁰ The parties to the proceedings should be able to challenge quality of the translation as well.⁹¹ The defence should have

87 *S. v Switzerland*, App no 12629/87 and 13965/88 (ECtHR, 28 November 1991) and art 4 of the Preamble of Directive 2013/48/UE, Commission, 'Report on the implementation of the Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty' COM(2019) 560 final.

88 Paweł Wiliński, *Rzeczelný proces karný w orzecznictwie sądów polskich i międzynarodowych* (Wolters Kluwer 2009) 26-27.

89 See also Luciano Cavalcante Siebert and others, 'Meaningful Human Control: Actionable Properties for AI System Development' (2023) 3 AI and Ethics 241.

90 *Kamasinski v Austria*, App no 9783/82 (ECtHR 19 December 1989), *Knox v Italy* App no 76577/13 (ECtHR, 24 January 2019), *Hermi v Italy*, App no 18114/02 (ECtHR, 18 October 2006).

91 *Kamasinski v Austria* (n 91).

sufficient means and opportunities to initiate review over translation or the interpretation. Therefore, there should be a clear possibility to analyse and recreate the mechanism of the system. If there is not – once again the effectiveness of the rights can be questioned.

Another major controversy, this time connected with the use of AI-based systems by the defence, appears due to the dynamic development of the systems created for the purposes of legal aid.⁹² These systems can be prone to malfunction as well and can constitute cause for deterioration in the situation of the defendant. Existing case law of ECtHR addresses the cases when the lawyer does not perform their duties in a diligent and active way. ECtHR sees these situations as a lack of effective defence. If the system, on which the defence was based, was in fact faulty, the result would be in fact the same. The question appears, what can be done to limit the possible threats and disadvantages, mitigate the negative effects, and finally if the systems should be subjected to any type of review.

Besides the elements included in art 6(3), the use of AI systems and lack of explainability can influence other elements of art 6 that are in fact strictly connected with effective execution of defence rights. One of the most prominent examples is reasoning of judicial decisions. According to case law of ECtHR, judgments of courts should adequately state the reasons on which they are based.⁹³ They should prove to the parties that the decision was based on objective arguments and demonstrate that they were heard. The reasoning of the court is also necessary to preserve defence rights.⁹⁴ Without it, it is impossible to fully exercise any available right of appeal.⁹⁵ When the defendant does not possess sufficient knowledge on the reasons that led the court to its decision, they cannot really challenge it and address it.

Lacking explainability can in fact cause serious deficiencies in reasoning of judicial decisions. When we take into consideration AI systems that assist in rendering a judgment, due to black box, the possibilities for presenting reasons on which the decision is based can be very much limited. The defendant may receive simply the result of the systems' workings, but not the real grounds in the commonly accepted sense. It is also connected with the limited abilities of the judge that is making use of AI systems. The possibilities for the defendant

92 Daniel Martin Katz and others, 'GPT-4 Passes the Bar Exam' (15 March 2023) 382 *Philosophical Transactions of the Royal Society A* (2024), <https://doi.org/10.1098/rsta.2023.0254> accessed 30 May 2024, <<https://openai.com/blog/chatgpt>> accessed 5 April 2023, <<https://firmsy.com/>> accessed 5 April 2023, <<http://www.billybot.co.uk/>> accessed 5 April 2023, <<https://blog.rossintelligence.com>> accessed 5 April 2023, <<https://donotpay.com/>> accessed 5 April 2023, <<https://robotlawyerlisa.com/>> accessed 5 April 2023.

93 *Moreira Ferreira v Portugal*, App no 19867/12 (ECtHR, 5 July 2017), para 84.

94 See 'Guide on Article 6' (n 81).

95 *Hadjianastassiou v Greece*, App no 12945/87 (ECtHR, 16 December 1992).

to challenge such decisions are in this case restricted and can affect the successful conduct of defence.

All these deficiencies combined can as a consequence influence the overall fairness of the proceedings. The ineffective rights cannot lead to a fair trial, which should be based on equality of arms and effective participation. According to case law of ECtHR, art 6 as a whole guarantees the right of defendant to participate effectively in a criminal trial.⁹⁶ It also includes a right to follow the proceedings.⁹⁷ Defence rights in their essence should contribute to implementation of these principles. It is a fundamental guarantee of the truly effective realization of the right to a trial. It grants the defendant the opportunity to choose their behaviour during the trial within the limits of the law, with the possibility of passive behaviour which is reflected in a privilege against self-incrimination, but also active participation in the proceedings and in taking steps to prove certain circumstances and present their version of events.⁹⁸ Without an adequate degree of explainability, this effective participation can be substantially restricted. Therefore, the proper regulation is clearly needed to safeguard the essence of right of defence.

3.4 Prospects for regulation

The need for imposing specific obligations on the public sector with regard to the AI use and explainability has been raised before, especially by the Council of Europe. The CAHAI (Ad hoc Committee on Artificial Intelligence) called for a legally binding transversal instrument that would include a series of provisions on legal safeguards applicable to AI systems used for the purpose of deciding or informing decisions impacting “the legal rights and other significant interests of individuals and legal persons”.⁹⁹ These safeguards should, at least, include the following: the right to an effective remedy before a national authority (including judicial authorities) against such decisions, the right to be informed about the application of an AI system in the decision-making process, and the right to choose interaction with a human in addition to or instead of an AI system, and the right to know that one is interacting with an AI system rather than with a human. The systems used should be trustworthy, ie intelligible, traceable and auditable. One general conclusion from these recommendations when applied to criminal proceedings is that the defendant should be able to take real actions and should be equipped with effective tools to challenge the AI-based evidence or decision process. To do so, they should be able to obtain all the relevant information, then understand it, and finally take proper measures.

⁹⁶ *Murtażaliyeva v Russia*, App no 36658/05 (ECtHR, 18 December 2018).

⁹⁷ *Moreira Ferreira v Portugal* (n 94).

⁹⁸ Stefan Trechsel, ‘The Right to Defend Oneself and to Have the Assistance of Counsel’ in Stefan Trechsel and Sarah Summers (eds), *Human Rights in Criminal Proceedings* (OUP 2006).

⁹⁹ CAHAI (n 41).

As for the scope of possible action for the defendant, there can be significant differences depending on the applicable model of the proceedings. In the adversarial models of the trial the defendant is equipped with a broader right to submit evidence gathered by private individuals, but must rely on his own or his lawyers' abilities in this regard. If the model is more inquisitorial, the evidence most likely will be obtained by the prosecutor and taken by the court. But in this case the question arises, if the defendant can effectively demand such information about the AI systems used. It has been emphasised before, that due to the fact that law enforcement agencies have a wide range of resources and the entire State apparatus at their disposal, the data acquisition rights are often one-sided in the proceedings where the new technologies are used. In such cases, there has been a visible trend of pre-trial phase domination in evidence collection. Also, due to the possibility of collecting data in a large amount and on a large scale, this leads to a situation, where defendant *de facto* has to prove his innocence.¹⁰⁰ This can be even more evident if the AI systems are used, as they can cause so much transparency issues that the defendant is not only burdened by them, but is not able to challenge them effectively.

Regardless of the model of the proceedings, defendant must be equipped with the effective means to obtain the data on the AI systems applied in the proceedings. Some interesting solutions has been introduced in the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (Proposal for the AI Liability Directive).¹⁰¹

According to the proposed Directive, Member States should ensure that national courts are empowered, upon the request of a claimant to order the disclosure of relevant evidence about a specific high-risk AI system that is suspected of having caused damage from a provider or a user. It is a significant facilitation for the claimant that gains access to the necessary tools for proving his statements. The Directive refers to the "evidence". However such a right to disclose the relevant information about AI systems itself could be attributed to the defendant. The ability to address the court and ask for the information on how the particular decision (both on the pre-trial and trial stage) was made with the reference to the inner workings of the system, could improve significantly the situation of the defendant.

If the ability to gather the information on the AI systems is guaranteed, then adequate measures should be introduced to guarantee the practical understanding of the files and effectiveness of the defence rights. However, different groups and entities will need different types of explanations.¹⁰² The needs of

100 Radina Stoykova, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence' (2021) 42 Computer Law & Security Review 105575.

101 Commission, 'Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence' COM (2022) 496 final (hereinafter 'Proposal for the AI Liability Directive').

102 See also The Royal Society, *Explainable AI: the basics Policy briefing* (The Royal Society 2019).

the court, huge legal companies and defendant acting on its own may not be the same. The assistance of experts should also be guaranteed in the proceedings – both for the use of the defence and the court. The defendant should be able to refer to the expert knowledge to effectively challenge the gathered evidence in case of any objections as to their reliability. The court should make use of such assistance of experts in case of any doubts connected with the evidence submitted by the parties to the proceedings, including the prosecution and suspected malfunctions in the systems.

As for the explainability models described above, the decompositional approach would be of great benefit for the experts. The use of eg surrogate models could assist the analysis and help really understand how the system reached its decision. Then, the processed information could be presented to the court and defence. Another way can be the strive for increased traceability. This is for example achievable by limiting the ways through which system decisions can be reached and creating a narrower scope for machine learning rules and features. This can reduce the problems connected with neural network hidden layers. It should represent more broadly the connections between individual neurons and the emerging internal dependencies between them. The example can be DeepLIFT (Deep Learning Important FeaTures), which identifies the activation of each neuron and its counterpart, thus allowing the reconstruction of the connection chain.¹⁰³

The decompositional approach is however of little importance for the defendant themselves. With no knowledge on the technology and the systems used, the defendant still does not understand to any extent, how the particular decision has been made – especially in the case of receiving the judgment and the particular penalty. If the AI systems are used on a large scale in the proceedings, it can result in decrease of general trust in the state. The solution can be the local interpretability (subject-centric approach). The defendant can gain insight into the grounds for particular decision, search for possible bias and draw the attention of the court to it.

Finally, in case of the use of AI systems for the benefit of the defendant, eg for the purpose of translation or to shape defensive strategies, the systems definitely should also be subjected to the review. Two situations can be differentiated – if the defendant uses the system on his own (especially not the free, publicly available one, but purchased) and if the system is provided to any extent by the state. In the latter case, the systems should unquestionably

103 Jon Rueda and others, ‘“Just” Accuracy? Procedural Fairness Demands Explainability in AI-Based Medical Resource Allocations’ [2022] AI & SOCIETY, Bas HM van der Velden and others, ‘Explainable Artificial Intelligence (XAI) in Deep Learning-Based Medical Image Analysis’ (2022) 79 Medical Image Analysis 102470, Avanti Shrikumar, Peyton Greenside and Anshul Kundaje, ‘Learning Important Features Through Propagating Activation Differences’ (*arXiv*, 12 October 2019) <<http://arxiv.org/abs/1704.02685>> accessed 26 April 2023.

undergo the introductory control process assessing their quality, with a view to the requirements of the AI Act. Moreover the defendant also should be able to initiate the review. If the AI system would be inefficient and malfunctioned, it should make an effective ground for an appeal. In the former, the systems also must be developed in accordance with the AI Act, however the potential consequences of the inadequacies and mistakes can be debatable. The defendant possibly could make use of the liability regime provided that the applicable conditions are met, but the ground for appeal is in this case very questionable as it can be perceived as the execution of free choice of the defendant.

4. Summary

Despite ongoing attempts to regulate the AI use in different spheres of legal and social reality, the AI systems' application in the criminal proceedings is still underregulated, particularly in the area of defence rights. The main aspect of the upcoming regulation should be safeguarding explainable AI as the black box is the biggest threat to the effective defence rights. The general need for xAI has been identified before - both in terms of public and private sector. However, it should turn into some specific obligations – both for the state and systems' developers.

In the current state of regulation the main threat is that the all the defence rights will not be effective. The AI systems' implementation into the proceedings does not result in the breach of any particular right *per se* at the first glance. They can be formally observed, but deeply ineffective. The decision made as a result of proceedings in which the information about the real nature of the evidence is in fact lacking, can be perceived as arbitrary and therefore contradict the aim of the AI use in the proceedings. Lacking information can further affect the ability to take real actions in the proceedings and issue any type of review. The review must be effective and accessible to the defence as there are considerable risks of bias and malfunction. They mostly have been raised in connection to the predictive policing, but can also affect other systems, for example ones based on NLP. Therefore to guarantee the effectiveness of defence rights, the explainable AI must be guaranteed. The explainability should be safeguarded by imposing obligations on the developers of the systems and implementing rights attributed to the defendant.

First of all, the legislator should ensure that providers of systems used in criminal proceedings strive for local interpretability and real explainability. The traceability of the AI –based systems should be ensured (to some extent introduced in the AI Act), but also means such as surrogate models should be disseminated. The general information about systems themselves does not give a proper extent of explainability sufficient for realization of the right to information. The main advantage of the local interpretability is that the defendant

themselves can gain insight into the reasons and premises for particular decision, which can help in retaining trust to the judiciary. The decompositional approach on the other hand and the use of surrogate models can be of great usefulness in cases where the review will be needed.

Then, the effective right to demand information must be introduced, possibly based on the Proposal for the AI Liability Directive example. The defendant should be given a clear right to challenge the results obtained by the use of AI systems with reference to the inner workings of the systems. To combine these two elements and guarantee the practical understanding of the files and effectiveness of the defence rights, the assistance of experts should also be guaranteed in the proceedings. The defence should be able to refer to such assistance and put AI-based evidence under their review and so should the court.

Finally, in case of the use of AI systems for the benefit of the defendant, the systems must undergo a proper review and should be labelled as high-risk. If the State is a provider of such system, the *a priori* review should be especially diligent. In case of any malfunction, it should make an effective ground for an appeal.

Some of the conclusions may appear overly future-oriented, however the rapid dissemination of the AI-based tools, such as ChatGPT, illustrates the possibilities for the AI systems create and can serve as a prognosis for the future. It is increasingly likely that the AI in some time will be commonly used in criminal proceedings. As a result, the legal act safeguarding the rights of the parties to the proceedings including the defendant should be issued. The one comprehensive regulatory act covering all spheres of application, such as AI Act, can be no longer perceived as sufficient in this case. In the criminal proceedings context, the most optimal and beneficial choice would be in this case a directive dedicated strictly to this sphere of AI use, as it would create a minimum standard for defence rights and at the same time it would leave some regulatory freedom to the Member States, allowing it to be adjusted to local needs and legal systems.

Determining the possible implementation of AI systems that can be compatible with procedural rights, including right of defence, is one of the key issues that judicial and law enforcement systems are going to face. It is also not without significance taking into account the field of European cooperation in criminal matters, mutual recognition of judgments and law enforcement cooperation. Significant system differences can significantly impede an effective response to criminal activities. Doubts concerning the systems assisting in rendering judicial decisions and lack of possibilities to review them can make it impossible to recognize such decisions in other EU Member States. As a result issuing such Directive could be beneficial for the international cooperation.

One final point to be made is connected with the issue of effectiveness versus the fair trial standards. The more complex the system is, the more concerns appear connected with transparency, explainability and, as a consequence, the

defence rights. It concerns eg unsupervised learning, AI systems based on artificial neural networks with hidden layers of nodes and deep learning. However, the more complex systems allow for higher efficiency and effectiveness. As a result, there is clearly a need for balancing the values – possible gain vs. human rights protection. The approach that the EU as well as Member States will choose – more guarantee or more gain-oriented will define the shape of regulation. As it can be drawn from the practice and recent statements of EU bodies, it appears that the EU has chosen the more protective approach and it will conduct harmonization based on the respect for human rights.¹⁰⁴ It can result in decrease in efficiency and slower development of the AI systems, but it will allow to safeguard the minimum standards arising from the provisions of the Convention, including fair trial standards and defence rights. Issuing the Directive with specific guarantees can prevent disregarding them by the particular States in favour of increased effectiveness and acceleration of the proceedings.

¹⁰⁴ Giovanni De Gregorio, in *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (CUP 2022), ch. 7 ‘The Road Ahead of European Digital Constitutionalism’.

*SECTION 4 – THE IMPACT OF DIGITALIZATION ON LEGAL
TRAINING*

What Every Law Student Should Know About Digitalization. Building a Digital Mindset for Future Lawyers

Per Andersen

University of Southern Denmark, Department of Law
ORCID 0009-0001-2945-3105

DOI: 10.54103/milanoup.215.c464

Abstract

In recent years, Danish employers have increasingly demanded lawyers who have insight into and understanding of the digital agenda. Often, however, the employers have not been particularly clear about what they are looking for, and therefore it has been difficult for the Danish universities to equip students with the skills and competences that an increasingly digitised labour market is looking for. Based on discussions and interviews as well as observations of other professions' desires, the author designed a course for the law programme, aiming at placing the first pieces of a legal digital mindset for the lawyers of the future. In the paper, the aim and pedagogy of the course and the gains that the approach so far seems to have given, is elaborated.

Keywords

Digitised Labour Market, Legal Digital Mindset, Education, Pedagogy

1. Introduction

In recent years, Danish legal employers have increasingly asked for lawyers who have insight into and understanding of the digital agenda. This is not special for the legal branch, but a common request from most branches hiring from, among others, higher education. But even though Denmark is usually categorized as one of the most digitized countries in the world, many employers are often not particularly clear about what they are looking for, ie, what they define as insight into and understanding of the digital agenda. This is also the case for legal employers which makes it difficult for the Danish universities

educating lawyers to equip the students with some of the skills and competences that the legal labour market is looking for.

Based on discussions and interviews with legal employers as well as observations of other professions' definitions of digital skills and competences, a colleague and I designed a course for the law programme at Aarhus University to lay down the first bricks of the students' legal digital mindset. The course ran for the first time in the autumn of 2022 and in the following, I will sketch the idea behind the course, the course lay-out, the teaching activities, and the students' evaluation of their new insights reached through the course. Doing this, the development of the course will probably seem much more straight-forward and rational than it was during the year it took us to find the right angle and set-up. Of course, as everybody developing courses within higher education knows, the process is never that straight-forward, especially not when you run a course for the first time. But following the course, I have become more and more convinced that we have found a concept which can function as a legal education's first step in building a digital mindset of the future lawyers. Hoping to inspire colleagues at other legal educations, I therefore want to use this possibility to share our ideas, set-up, and experiences.

To begin with, I will introduce the frame for legal educations and the legal labour market in Denmark, including a short introduction to the highly digitized public and private sector. This is done to provide the major context for the course and the decisions on what subjects to be covered and to what degree they should be covered.

Following this, in part 2, I will discuss the main problem in designing the course, ie, identifying what the legal employers specifically are asking for. I will also reveal how we came to think about a digital mindset and broader competences instead of more hardcore IT skills, which is, I think, the often-misunderstood solution chosen when we as teachers and educations are asked to deliver some solutions to the requested digital skills and competences.

In part 3, I will introduce the main idea in Paul Leonardi and Tsedal Neeley's book *The Digital Mindset* from 2022,¹ which gave us the frame for developing a teaching model for the course, and how I supplemented it with a legal 'leg' to make it a professional legal digital mindset.

In part 4, I will give an insight into the teaching activities and the pedagogical choices made and connect the activities to the model for a legal digital mindset introduced in part 3.

And finally in part 5, I will shortly go through the students' evaluation of the course and judge to what degree we succeeded.

1 Paul Leonardi and Tsedal Neeley, *The Digital Mindset. What it really takes to thrive in the age of data, algorithms, and AI* (Harvard Business Review Press 2022). It is Leonardi and Neeley's aim to help business managers transform their businesses to the digitized world, but the principal points, I think, can be used in every process aiming at digital transformation.

2. The Danish context

As indicated above, the classic mono-professional legal education in Denmark takes place at some of the public funded universities. There are eight universities in Denmark, each one with their individual academic, regional and historical profile. While some of them are mono-professional universities centred on IT, technical sciences, or business, four of the five academically broader and geographically spread universities offer a law-degree. Although the universities' main campuses are located in the capital and the largest cities of the country, the universities are present with both research and education across the entire country due to local campuses.² These years, this de-centralising organisation are to some degree strengthened as the former Danish government pushed the universities and other higher educational institutions to develop further educations in some of their minor campuses in order to offer more educations at a local level.³ Thus, four of the five broad universities offer a full classic education in law, ie an undergraduate, a graduate and a doctoral programme.⁴ From autumn 2023, one of the universities will also offer a legal education in the country's fifth-largest city due to the political initiative to go as local as possible.⁵

The geographically de-centralised structure of the legal educations in Denmark gives the universities the opportunity to be in contact not only with central organisations representing the profession and larger employers, but also with lawyers from both major and minor law firms, companies, and lawyers from different divisions of the public sector. In general, this should give the universities the possibility to get a broader picture of the development of the labour market and what the employers are asking for across the country.

The number of active Danish university educated lawyers has sextupled during the last century from 3,363 in 1928 to 19,659 in 2017.⁶ The number increased particularly during the formative years of the Danish welfare state following World War II as lawyers made up major part of the academic employees in the growing public administration. Since then, other professions have slowly

2 Universities Denmark, 'Universities Denmark' <<https://dkuni.dk/?lang=en>> accessed 21 April 2023.

3 Ministry of Higher Education and Research, *Tættere på - Flere uddannelser og stærke lokalsamfund* <<https://ufm.dk/publikationer/2021/filer/taettere-pa-flere-uddannelser-og-staerke-lokalsamfund.pdf>> accessed 21 April 2023.

4 Ministry of Education, 'Uddannelsesguiden: Jura' <<https://www.ug.dk/uddannelser/bachelorogkandidatuddannelser/bacheloruddannelser/samfundsvidenskabeligebacheloruddannelser/forvaltningmv/jura>> accessed 21 April 2023.

5 Ministry of Higher Education and Research (n. 3), 14.

6 Ole Hammerslev, 'At studere juridiske eliter' <<https://www.sdu.dk/da>>, 3-4, and The Ministry of Employment, 'Svar på spørgsmål til Folketingets Uddannelses- og Forskningsudvalg 5.10.2017' <<https://www.ft.dk/samling/20161/almdel/ufu/spm/181/svar/1431436/1799086/index.htm>> accessed 22 April 2023.

gained in and taken over the lawyers' domain in the public administration, but still, lawyers make up approximately one-third of the academic workforce in the public sector. Numbers from the last century show a steady development with approximately 30% of the educated lawyers working in the public administration while approximately 30% are working as lawyers in private law firms. The rest, ie, approximately 40% and slightly increasing since the 1980s, has found other domains for their expertise, eg, as in-house lawyers at major business companies, accountancy firms etc.⁷

In Denmark, the title 'jurist' is not a protected title as it is only referring to a person giving legal advice, but usually it is only used by and for people educated in law from a university. No matter whether you are a professional judge or lawyer, an in-house jurist or public servant, lawyers in Denmark are not educationally specialised in one or another legal field. All legal university educations in Denmark are generalist educations as laid down by the national Educational Act.⁸ While tasks as in-house lawyers at major business companies or accountancy firms may also be handled by university educated Masters of Science in Business Administration and Commercial Law (cand.merc.jur.) – an education combining business economics and administration with commercial law dating back to the business schools of the 1980s⁹ – or others, the tasks as lawyers and judges can only be handled by the jurists having obtained a five-year degree in law from a Danish university (cand.jur.). Hence, according to the Danish Administration of Justice Act, the classic cand.jur. degree is needed in order to gain the right to appear before the court or become a judge in court.¹⁰ From time to time, it has been discussed if Masters of Science in Business Administration and Commercial Law should be allowed to practice as barristers and solicitors, but in fall 2021 this was once again rejected by the Ministry of Justice, apparently due to a lack of sufficient specialised knowledge of law.¹¹ It

7 Hammerslev (n. 6), 6.

8 Ministry of Higher Education and Research, 'Bekendtgørelse om universitetsuddannelser tilrettelagt på heltid' App.1: 3.1 <<https://www.retsinformation.dk/eli/lta/2020/20>> accessed 22 April 2023.

9 Copenhagen Business School, 'En uddannelsessucces fylder 30' (2014) <<https://www.cbs.dk/presen/nyheder/uddannelsessucces-fylder-30>> accessed 22 April 2023.

10 Ministry of Justice, 'Bekendtgørelse af lov om rettens pleje' § 42, stk. 3 (concerning judges), and § 119, stk. 3 (concerning lawyers) <<https://www.retsinformation.dk/eli/lta/2021/1835#idabd7a4b3-43d2-477e-9e29-06e6df4105ea>> accessed 21 April 2023. See also 'The European Union, 'European Justice: Denmark' <<https://e-justice.europa.eu>> accessed 22 April 2023. To be allowed to act as a lawyer before court, ie, as barrister and solicitor, the theoretically educated classic jurist (cand.jur.) must also pass a test approved by the Minister of Justice. This consists in a three-year long practical training at a law firm, a practical test of how to handle legal cases and processes, and a theoretical test of the task and ethics of a lawyer, cf Ministry of Justice (n. 8), para 119.

11 Copenhagen Economics, 'Competition and regulation of the legal Sector in Denmark' <<https://www.copenhageneconomics.com/dyn/resources/Publication/>>

is possible for the *cand.merc.jur.s* to get the right to appear before the court if they supplement their education with a two years programme of law, but no doubt, the question whether they can act as barristers and solicitors following their degree will arise again within a few years as the major law firms are now increasingly hiring also *cand.merc.jur.s*. It seems that the firms do so both because of a lack of classic lawyers and because people with a combination of law and business administration usually understands business better, including the business need for digitalization. This, of course, in the long run puts pressure on the mono-professional classic lawyers and their monopoly.

While approximately 30%, ie, 7000 of the classic lawyers are working within the public sector, the same number work as lawyers, including in-house lawyers with the right to represent their firm in court.¹² The vast majority of lawyers used to be organized in small to medium-size firms, but during the last decade, two handful of domestic firms offering full legal services have become more and more dominating in the Danish legal market. This is the firms now hiring also Masters of Science in Business Administration and Commercial Law, working on expanding their understanding of and services within business in a broader sense, often including developing digital services both to in-house processes and for their customers as self-run services. It is important, though, to stress that none of the two legal-orientated educations have mandatory courses focusing on digitalization for the time-being, but at some of the educations, such courses are underway, while other educations still offer them as optional courses as part of the individual student curriculum.¹³

The existing lack of the development of digital skills and competences as a mandatory element in Danish law-programmes may come as a surprise as Denmark is ranked one of the most digitized countries in the world.¹⁴ Denmark has a well-functioning digital infrastructure, both when it comes to high-speed internet connections throughout the country and digital access to all public services. According to the Danish Ministry of Culture, in 2019 99% of the Danish households had access to the internet by either a mobile phone or a computer (ie, a laptop, desktop or iPad device), including 93% of the citizens aged 71 or older. Almost all Danes, namely 91%, use the internet daily and another 6% on a weekly basis, which makes the internet one of the most used platforms for

publicationPDF/7/287/1430739706/competition-and-regulation-of-the-legal-sector-in-denmark.pdf> accessed 22 April 2023.

12 The Danish Bar and Law Society, 'The Danish Bar and Law Society' <<https://www.ad-vokatsamfundet.dk/english/about-us/>> and The European Union, 'European Justice: Denmark' <<https://e-justice.europa.eu>> accessed 22 April 2023.

13 The education in law at University of Copenhagen offers more optional courses, and from 2025, the bachelor in law at the University of Southern Denmark will contain the first mandatory course on fundamental digital skills.

14 European Commission, 'The Digital Economy and Society Index (DESI) 2022' <<https://digital-strategy.ec.europa.eu/en/policies/desi>> accessed 22 April 2023.

information and contact among the Danes.¹⁵ Most public services are reached through the gateway 'borger.dk', that is 'citizen.dk'.¹⁶ This is supplemented by specialised websites for tax, a mailbox where the individual citizen receives all relevant public communication etc.¹⁷ The Danish Parliament has also decided that the public administration must digitize as much of the administration as possible every time a new law has been passed by the Parliament.¹⁸

The Network Readiness Index, which measures and ranks countries globally on the digitization of their economies, yearly positions Denmark as one of the most future-ready societies.¹⁹ The ICT sector is one of the fastest growing sectors in Danish economy and has strong attention and support from the Danish government, which at the beginning of 2021 took the initiative to establish a political-strategical partnership between the public and private sectors in order to ensure that Denmark would proceed its digital development.²⁰ With the prevalence of ICT use and the government's wish to continue the development of making Denmark a hub for innovative multimedia technology, it must be expected that the need for digital skills and competences will only grow in the coming years, including lawyers' understanding of how digital tools function and affect the public sector as well as private business.

This goes hand in hand with the development within the Danish court system which has also embraced the new digital possibilities. Nowadays, it is possible to file a lawsuit and record summons, defences, and other pleadings, or to record appeals and requests for reopening of cases etc. via a digital portal,²¹ just as digital registration of a deed was implemented at the Land Registration

15 Ministry of Culture, 'Internetbrug og enheder 2020' <<https://mediernesudvikling.kum.dk/2020/internetbrug-og-enheder/>> accessed 22 April 2023.

16 Ministry of Finance at <<https://www.borger.dk/#>> or <<https://lifeindenmark.borger.dk/>> accessed 22 April 2023. For an introduction to many of the systems, see <https://en.digst.dk/> accessed 27 April 2023.

17 See eg the Danish Customs and Tax Administration at <<https://www.skat.dk/>> accessed 22 April 2023.

18 Hanne Marie Motzfeldt, Jøren Ullits and Jørgen Kjellerup, *Fra forvaltningsjurist til udviklingsjurist – Introduktion til offentlig digitalisering* (DJØF Forlag 2020), 60-63. See also Agency for Digital Government, 'Digital-ready administration' <<https://en.digst.dk/>> and Regeringen, KL, Danske Regioner, 'Digitalisering, der løfter samfundet. Den fællesoffentlige digitaliseringsstrategi 2022-2025' <https://fm.dk/media/26022/digitalisering-der-loefter-samfundet-den-faellesoffentlige-digitaliseringsstrategi-2022-2025_web.pdf> accessed 21 April 2023.

19 The Network Readiness Index 2022, 'Denmark' <<https://networkreadinessindex.org/country/denmark/>> and <<https://networkreadinessindex.org/>> accessed 22 April 2023.

20 Ministry of Finance, 'Nyt digitaliseringspartnerskab skal bringe Danmark og danske virksomheder ud af coronakrisen og stærkere ind i fremtiden' (2021) <<https://fm.dk/nyheder/nyhedsarkiv/2021/marts/nyt-digitaliseringspartnerskab-skal-bringe-danmark-og-danske-virksomheder-ud-af-coronakrisen-og-staerkere-ind-i-fremtiden/>> accessed 22 April 2023.

21 The Courts of Denmark, 'A Closer Look at the Courts of Denmark', 18 <<https://domstol.dk/media/jqhg2psf/a-closer-look-at-the-courts-of-denmark.pdf>> accessed 22 April 2023.

Court half a decade ago.²² The administration of the Courts of Denmark has also published a new central database that gives all citizens free access to judgments delivered by the courts. This database contains judgments based on fixed principles of essentiality and it will continuously be updated with new rulings. Moreover, the database will contain historic rulings from civil and criminal cases of public interest.²³ At the same time, courts are increasingly embracing ICT through the introduction of videoconferencing, but it is introduced cautiously and only in certain matters.²⁴ The same wariness is so far also seen concerning the possible use of AI in the court system.²⁵ According to the international WJP Rule of Law Index, this well-considered development has placed Denmark as one of the legally most well-functioning states the last couple of years.²⁶

This development towards more and more digitized services is not only seen within the public sector, but also within the private sector.²⁷ This includes legal services. Thus, one of the major Danish law firms has established a legal tech division developing digital administration, management, and legal service tools for their customers, while other law firms focus on advising on standard digital systems and solutions.²⁸ Most of the law firms are also focusing on developing (or buying) digital tools to optimize their internal working processes.

3. The problem: designing a course on digital skills and

22 The Courts of Denmark, 'The Danish Judicial System' <<https://domstol.dk/om-os/english/the-danish-judicial-system/>>, <<https://domstol.dk/tinglysningssretten/>> and <<https://www.tinglysning.dk/tinglysning/landingpage/landingpage.xhtml>> accessed 22 April 2023.

23 The Courts of Denmark, 'A Closer Look at the Courts of Denmark', 18, concerning 'The Courts of Denmark, 'Domsdatabasen' <<https://domsdatabasen.dk/>> accessed 22 April 2023.

24 Ministry of Justice, 'Rigsadvokatmeddelelsen, Brug af videolink i retsmøder' <<https://www.retsinformation.dk/api/pdf/209129>> accessed 22 April 2023.

25 cf the comment by the director of the national board developing the courts' work (Domstolsstyrelsen) <<https://www.altinget.dk/artikel/domstolsstyrelsen-kunstig-intelligens-afsloerer-fordomme-mod-koen-og-hudfarve>> and the European Commission for the Efficiency of Justice (CEPEJ), 'European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment' <<https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>> accessed 21 April 2023.

26 World Justice Project, 'Rule of Law Index 2022' <<https://worldjusticeproject.org/rule-of-law-index/global>> accessed 22 April 2023. This is the case, even though there is a growing criticism of the expenses and the chances for winning if you are suing the government and public administration, cf DJØF, 'Borgernes retssikkerhed i sager mod det offentlige' <https://www.djoef.dk/-/media/documents/djoef/j/jurapanelets-undersogelser/jurapanel_unders-oe-gelse_a4_1021_borgernes_retssikkerhed_korr2.ashx> accessed 22 April 2023.

27 cf Ministry of Industri, Business and Financial Affairs, 'Redegørelse om Danmarks digitale vækst 2022' <<https://www.em.dk/>> accessed 22 April 2023.

28 See eg <<https://www.bechbruun.com/da/legaltech>> and <<https://www.horten.dk/specialer/it-ret-og-telekommunikation>> accessed 27 April 2023.

competences

Even though public as well as private legal employers are going more and more digital, both when it comes to their internal working processes and in the services offered to citizens and clients, it has been difficult to identify which digital skills and competences they in general are asking for from newly educated lawyers. For half a decade I have talked to employers and lawyers, and I have participated in different working groups and task forces trying to identify the digital skills and competences asked for in order to implement them in our educational activities. To my experience, it has been difficult for the legal employers to put words on what they are asking for specifically, probably because it is not always clear to them either as they, or we as a society, are in a continuously ongoing process when it comes to digitalization. It is not, that they have not tried to put some words on through, for example, the employer panels connected to every legal education, or working groups initiated by, among others, the Confederation of Danish Industry.²⁹ But usually, it has been formulated in broad terms which we at the legal educations have not been able to use as a starting point for specific learning activities, even though the good will has been there.

Hence, in 2020 several Danish universities founded the common project 'The Digital Curriculum' with the aim of identifying the skills and competences asked for within the social sciences and the humanities and thereafter develop the teachers' skills needed to fulfil the requests.³⁰ At the same time, the Faculty of Law at the University of Copenhagen and the IT University of Copenhagen joined forces to develop a basic tech course for university (and especially law) teachers.³¹ Both projects were funded by the Danish Ministry of Higher Education and Science and thus placed the question of the teachers' digital skills in the strategic educational agenda. As far as I know, none of these projects have been able to identify in detail what the legal employers are asking for, at least not in a way that can be transferred into specific teaching activities within an educational frame.

29 See eg the Confederation of Danish Industry, 'Kompetencer til et digitalt erhvervsliv' <https://www.danskindustri.dk/globalassets/tech-der-taller/digitale_kompetencer_pjece_2020-009.pdf/Download> and 'Behov for digitale kompetencer hos samfundsvidenskabelige kandidater' <<https://www.danskindustri.dk/arkiv/analyser/2022/4/behov-for-digitale-kompetencer-hos-samfundsvidenskabelige-kandidater/>> accessed 27 April 2023.

30 See The Digital Curriculum at <<https://digitalcurriculum.au.dk/>> accessed 27 April 2023.

31 IT University of Copenhagen, 'Ny bevilling: Digitalt løft af undervisere skal opruste samfundet med it' <<https://www.itu.dk/om-itu/presse/nyheder/2020/ny-bevilling-digitalt-loeft-af-undervisere-skal-opruste-samfundet-med-it>> accessed 27 April 2023. Parallel to this, the Faculty of Law founded the Copenhagen Legal Tech Lab, cf. <<https://jura.ku.dk/legaltechlab/>> accessed 27 April 2023. The Lab mainly focuses on research and knowledge share, especially on the technical development and its possible implications for law.

So, on the one hand it has been difficult for the legal employers to put words on what they are asking for without doing this in broad terms, and on the other hand it has been difficult for the educations to decipher what the employers are asking for. The main problem seems to be that the legal employers are not asking for the skills that we at the universities are used to provide, namely classic legal skills. Therefore, it has been and is difficult for the highly specialized legal university milieu to translate the words and the cases used by many of the employers into learning activities, because in the essence, the employers are not asking for typical legal skills when it comes to digitalization. Thus, for a highly specialized academic legal professor at a university, it is impossible to transfer the often broader and more business minded competences asked for into meaningful teaching activities in a legal course.

In short, as far as I can conclude from my talks with employers and reading of reports and contributions to the debate, the skills asked for by the Danish legal employers can be summed up in a couple of handfuls of broader, not very specified – and not very classic legal – competences.

The most specific or detailed input has come and still comes from the public employers, probably due to the sector's volume and the fundamental digitalization of its services based on a common strategy. Hence, the public employers wish that the newly educated lawyers have a basic knowledge of the sector's digital landscape, ie, the structure of and division between national and local services, and who has the task or competences to handle which subject fields. At the same time, the lawyers must have a basic understanding of how computers work and of different digital technologies to make them understand not only the scope of a digital project, but also the possible legal problems or possibilities with the technology at hand. Thus, the future lawyers must be able – or at least interested in – talking to other professions such as IT-professionals. To be able to do so, one of the common broad competences asked for is knowing something about working in cross-disciplinary projects, eg, from the public sector's procedural model for IT-projects or through practical projects during the education.³²

The public employers, that I have spoken to, have all mentioned that for a jurist working in the sector, it is of course necessary to know administrative law and GDPR. But they have stressed that this is not enough for the future. Thus, they are looking for lawyers who, of course, have the classic legal skills to be able to participate in developing, buying, adjusting, and using digital solutions – and to complain if they are not working as expected. But nowadays, the employers stress that the technological solutions and possibilities are so complex that it is necessary for those taking care of law to have a basic understanding of

32 The Danish Agency for Digital Government, 'Statens it-projektmodel' <<https://digst.dk/>> accessed 27 April 2023.

the technology for them to solve their tasks in a proper way. Especially when it comes to the development of digital services or in making digital-ready legislation. Lawyers are the safeguards of rule of law and to keep on being this, they need to know what can happen when you digitize law and services within the public sector, the mantra seems to be.

Compared with the public sector, the private legal employers such as law firms and in-house lawyers are not as specific when it comes to digital skills and competences. They are mainly concerned with one thing, that is business. Time is money and therefore they are eager to make their working processes more efficient, wishing for the new lawyers to be able to participate in the development of digital tools to automate the company's internal working processes. The Danish market for legal services has not yet been liberalized in the same manner as, for example, in the United States or Great Britain,³³ and therefore the law firms are not yet under the same pressure to develop new services as abroad. But some of the major law firms are looking into developing new digital legal products and offer them as semi-automated services to their clients. Therefore, they ask for lawyers able to identify such possible new products, knowing that the market and their business model may soon change.³⁴

In short, the Danish legal employers seem to be asking for lawyers having a basic understanding of how computers work and of different digital tools and technologies. Besides this, the lawyers-to-come must to some degree master the four general competences characterized as 'the 21st century skills', that being critical thinking, communication, collaboration, and creativity. All competences that we have not until now been used to or very focused on developing at a typical Danish legal education.

Looking into this context, my colleague and I decided to frame our plans for a course focusing on digital skills and competences to be run at the legal education at Aarhus University in an, from an academic perspective, unusual way: We framed the course around the lawyers' tasks in a digitized job market, ie, we decided to develop a course about the practical side of working as a lawyer in a more and more digitized society. By doing so, we had a frame that

33 See eg Richard Susskind, 'Tomorrow's Lawyers' [2013] *Law Practice* 34; Dan Hunter, 'The death of the legal profession and the future of law' [2020] *University of New South Wales Law Journal* 1199; Chay Brooks, Cristian Gherhes and Tim Vorley, 'Artificial intelligence in the legal sector: pressures and challenges of transformation', [2020] *Cambridge Journal of Regions, Economy and Society* 135.

34 As concluded in, eg, reports by the The Danish Bar and Law Society, that is Advokatsamfundet, *Legal tech og advokatregulering* (2019) <<https://www.advokatsamfundet.dk/publikationer-og-boger/rapporter-og-vejledninger-1/legal-tech-og-advokatregulering/>>; the major law firm Bech-Bruun, *Inhouse-juristens nye digitale virkelighed. Et indblik i anvendelsen af legaltech i danske virksomheder* (2022) <<https://www.bechbruun.com/>>; and the yearly Karnov Group, *Brancherapport 2021* <<https://www.karnovgroup.dk/fremtidens-jurist-2021>> 63-86. All accessed 27 April 2023.

made it possible to have both digital learning activities on a knowledge basis, activities focusing on broader competences such as working in projects with IT-professionals, and space for reflecting both critically and innovative on the use of digital technologies, not at least compared to rule of law. As the idea developed, it turned out that we were not just interested in law, technology, or broader competences, but in laying the first bricks to, a basis for, a legal digital mindset for the lawyers of the future.

All we could achieve within a single basic course, we realised after having read Paul Leonardi and Tsedal Neeley's book about *The Digital Mindset*, which one of my colleagues working with digital transformation in business recommended, was that the students knew enough about digitalization and working with digitalization to be open-minded towards participating professionally in the digital transformation of law and society. Hence, it became our main aim that the students participating in the course would take the first steps to become an active part in the process of digitalization and that they would develop ability to reflect on digitalization from a lawyers' view.

4. Developing a teaching model for a legal digital mindset

The basic idea in Paul Leonardi and Tsedal Neeley's book from 2022, *The Digital Mindset*, is that you only need to understand 30% of each of three focal points to lay down the first steppingstones for a digital mindset which then can be further developed.³⁵ The book, in a language understandable to laymen, presents what these 30% is which makes it a usable hands-on presentation for those of us not well acquainted with the fundamentals of digitalization. The three focal points that Leonardi and Neeley are working with, are what they call the three "Cs": Collaboration. Computation. Change.

The first, Collaboration, is about understanding what computers can and cannot do.³⁶ Leonardi and Neeley introduce how computers work, including the basic ways of Artificial Intelligence (AI). By doing so, they give the reader a vocabulary and set of concepts to work with which makes it possible both to understand the limitations of digitalization and to communicate, at least on a basic basis, with others about digitalization. This includes an understanding of the limits of AI and machine learning as tools which often cannot give exact answers, but only probabilities.

Leonardi and Neeley's second C, Computation, is about understanding what data is and what the problems with data can be.³⁷ The main point here is that data is something that we produce depending on what information we want to

³⁵ Leonardi and Neeley (n 1), 1–12.

³⁶ *ibid*, 25–50.

³⁷ *ibid*, 73–96.

capture and how we categorize it. This includes a critical approach in identifying, analysing, and concluding on data, being aware of possible biases in both humans and machines; the latter especially when it comes to machine learning.³⁸

The third C is Change. While Collaboration and Computation is mainly focusing on the technical or systematic-analytical sides of digitalization, Change is concentrated on the societal and mental frame for digitalization. This includes how to handle possible biases between, eg, cybersecurity and privacy,³⁹ and how to remove mental barriers of distrust towards the digital to replace it with a constructive and curious, but still critical thinking.⁴⁰ As Leonardi and Neeley are aiming at helping business managers in transforming business to adapt to a digitized world, they link the technical-analysing knowledge and understanding with the mental change needed, if you want to succeed with digital transformation. This link is important, because it stresses that change is not coming from the computers, but from us humans. Digitalization is also a human process.

With the help of the three C's, my colleague and I were able to identify what the students basically needed to know about digitalization from a technical viewpoint, but also that it, at the end of the day, was about changing the way they were thinking about it, no matter whether they addressed the digital development sceptically or positively. Realizing this, we took it further due to the professional tasks of lawyers and supplemented the three Cs with three legal subject-specific focal points centred around three "Us": Understanding the legal-normative framework for digitalization; Understanding the organisational framework for lawyers' work with digitalization; and Understanding the legal-ethical challenges of digitizing the legal field. By doing so, we turned Leonardi and Neeley's digital mindset into a *legal* digital mindset.

What we wanted to gain with the first U focusing on understanding the legal-normative framework for digitalization was to make the student acquainted with both the Danish and the international regulations on digitalization, ie, the legal frame that they will have to know and work within in the future. This, of course, is mainly GDPR and the Danish Parliament's decision to work for digital-ready legislation. But our focus was not so much on the rules themselves, but on the principles and concepts and, foremost, on making the students interested in following the current development within EU regulation and principal cases on GDPR such as Chromebook, Google Analytics etc. The fundamental idea was that as a lawyer working with digitalization – or maybe as a lawyer in general – it is not enough to know the existing rules, but also to be able to, to some degree, foresee what is coming when it concerns the digital development.

38 To pinpoint that one has to be aware of the difficulties in using machine learning, Leonardi and Neeley even gives a short introduction to statistics, cf *ibid*, 97–115.

39 *ibid*, 119–143.

40 *ibid*, 145–196.

The second U – Understanding the organisational framework for lawyers' work with digitalization – involved understanding the organization of and the main drivers in both the public and the private sector. We wanted the students to be acquainted with the public sector's digital landscape such as the division between national and local services, and who has the task to handle which subjects. But we also wanted them to know the strategic goals of the sector as these had developed over time and are formulated in the current common strategy. This also involved tools such as the sector's procedural model for IT-projects or manual for developing digital-ready legislation. Concerning the private sector, the students then had to understand the traditional business model of law firms, and what was driving the digital interest and development within that sector, including the possible threat to the existing business model if the Danish private legal sector will be liberalised sometime in the future.

The final U was focusing on Understanding the legal-ethical challenges of digitizing the legal field. This involved understanding and being able to reflect upon digitalization as a tool to make, eg, public administration more effective vs the task of securing rule of law for the citizens. The aim with this U was to make the students aware of the grey zones derived from digitalizing especially the public sector and to make them able to approach the problems in a constructive way in order not to just put the development of digital services to a halt, but to be participating in digital projects as a core member. This involved being able to work in cross-disciplinary projects and to communicate with other professionals, especially IT-professionals, being aware of what they knew as lawyers and in which subject fields they were not the specialists. This U also involved knowing the ethical norms for lawyers and the institutional setup for enforcing them within the private sector.

In the course, we used the three Cs and the three Us as a frame for the teaching activities, both to clarify what they would learn something about during the course and to make it clear why we had picked the subjects and chosen the activities that we had. Every class opened with an introduction to which of the Cs and Us we would investigate today and, in this sense, the three Cs and the three Us formed a teaching model that made the interaction between technology, law, everyday work life as a lawyer, the mental preparedness to get involved in digital projects, the institutional frame one is working within etc. clear to the students.

Concerning the exam, we had an individual oral discussion based on an individually written assignment. The assignment consisted of an analysis of a self-picked case involving both a legal part and a practical-digital part, and in the assignment the student should also reflect on how to proceed to solve or further develop the subject of the case. By drawing on the students' knowledge and ability to analyse a current case, we wanted to push (and in the exam of course to test) their ability to identify both problems and possible solutions and

to reflect on digitalization as an ongoing process involving also legal subjects and thus, also lawyers.

5. Teaching activities

The aim of the course made it clear that we were going to do something different than usual (which, at least in a Danish context, is often reading legal sources and literature, maybe training in solving cases on the subject). At the same time, we realized that most of the subjects would need comprehensive cross references because of their close-knit connections and the literature available, illustrating exactly the close connections. The decision to do something different than usual was strengthened by the fact that the course was open for participants from both the classic legal education and the Master of Science in Business Administration and Commercial Law which gave a diverse academic grounding; a diversity that we wanted to use constructively in pushing the students to be professionally more open-minded than they often are following three or four years of study.

Hence, we decided to make use of and mix different sources and elements from class to class, both when it came to the texts to be read and to the more practical activities and discussions run during class. Therefore, the main structural decision was, as mentioned above, to begin every class with an introduction to today's main subject and how the program of today related to one or more of the Cs or Us. Besides this, it would be necessary to read some academic literature for every class, but this was often supplemented with public strategies or manuals, relevant regulation, reports or webpages about current cases etc. We had, as eye-openers, simple practical exercises in excel, showing the problems with unreliable data in the simplest way possible, and an exercise where we tried to develop a pseudo-code for one of the simplest criminal Danish laws to illustrate how difficult it is to develop a code able to contain all possibilities and thus give an authoritative solution to a legal problem; by doing this, we opened for a discussion about whether digital tools can be used as decision-makers or just as supportive tools for human decision-making. We identified relevant podcasts or podcast programmes to listen to in-between classes, both as a background for discussions and to show that the question about law and digitalization is highly debated and constantly changing. And finally, we invited practitioners – that being lawyers, IT-professionals, and specialists in strategic development of business administration – to share their experiences with practical life in implementing or developing digital solutions, eg, how to implement GDPR in the police force, how to develop digital tools to automate work processes within law firms, how to develop public services in the tension between administrative efficiency and rule of law, how to overcome the gap between lawyers and IT-professionals etc.

Every class had its own heading to address some of the subject fields asked for by the legal employers. Concerning public digitalization, we addressed digital strategies, administration directed towards the citizens, the digitalization of courts and online dispute resolutions, digital-ready legislation, and the role of the lawyer in digitalization projects. Regarding the private sector, we specifically addressed task and project management. These subjects were supplemented with more general subjects on digital technologies, ie, how to code (including the exercise of pseudo-coding, not real coding) and a short introduction to technologies such as machine learning, blockchain etc., on data quality and cybersecurity (including GDPR), the historical development of digital technologies and the changing role of lawyers, including lawyers' ethic in a development focusing on efficiency.

As illustrated with this short outline of the activities in the course, we did not go deep into any specific subject. The set-up was based on giving the students an understandable frame and good grasp of what digitalization is, what the technical possibilities and challenges are, how the subject area is regulated by law or misses regulation, and how they as lawyers can participate constructively in digital projects at the same time as they maintain their role as lawyers, focusing on rule of law. The aim was not to make digital experts out of them, but to prepare them for the digital job market that they are entering after graduating. The aim was to lay down the first steppingstones for a critical-constructive way of thinking about digitalization, so that they would be able not just to participate in digital projects, but maybe even take lead in a legally proper development of digital solutions.

6. Evaluation and reflections on the future development

At the core of all these activities and the reason for arranging the course was that we wanted the students to get and develop a basic understanding of both the technical, the organisational, the professional, and the individual level in the process of digitalization in the legal job market. We wanted the students to become able to participate constructively, but professionally reflected in digital projects. Following the course, they should neither be afraid of digitalization nor be so positive and eager to streamline, eg, the public administration that they lost sight of rule of law.

To know whether we succeeded or not, we had a colleague specialized in evaluations to evaluate both during the course to see if we were on track, and following the last class as we were interested in their reflections before exam hit them. And then, of course, we could see how the exam worked out.

Both the assignments, the grades, and the feedback from the students indicated that we succeeded. The students told us that the course had helped them de-mystifying most aspects of, and provided them with a language to talk

about, digitalization. In addition to an understanding of the technical digital Cs, the students felt that they had got an understanding of the mental, professional-social, and professional context that is part of the digitalization process. Furthermore, they had got an understanding of the principles behind data protection, but also how these challenges the digital opportunities (in relation to data transfer to third countries etc.). As a bonus to the Us, the students also indicated that they had gained a fundamentally better understanding of the rule of law due to the discussions about effective digitization vs rule of law and due process. Thus, they simply felt better prepared to assess advantages vs disadvantages in the digital development taking place and to identify and react professionally on the tension between efficiency and law.

We did not reach the 30% mentioned by Leonardi and Neeley, though. In that sense, we did not succeed, because we simply did not have the hours needed to make the 30%. We prioritized to reach approximately the first 10% and then spent time to develop a digital legal mindset instead. And this time was well-spent, I think, because it showed that the 10% of the three Cs was necessary to know something about, even for a lawyer. Through the course, the three Cs did not show all that you may need to know about digitalization, but the Us showed that you even as a lawyer need to know *something* about digitalization – and that was a huge factor for the students' motivation through the course. In that sense, I think that we laid down the fundamental steppingstones for a legal digital mindset to be further developed. In all modesty, I think that we succeeded in identifying the minimum of what every law student should know about digitalization.

Law in the Age of Digital Technologies

Edited by Francesca C. Villata, Mirela Župan, Katarina Trimmings,
Giulia Gabrielli

The widespread use of digital technologies and the rise of the information society bring about significant transformations and social changes that impact law and legal skills. In light of these extensive digital shifts permeating every facet of our society, this volume acknowledges the need for enhanced clarity and provides insights into a wide array of substantive and procedural legal issues. These include the international legal regulations governing state conducts in cyberspace, as well as matters related to the private realm of digitalization, where cross-border business transactions and personal rights alongside family matters present unique challenges and concerns. Finally, the volume also addresses how digitalization influences legal education.

Time to Become Digital in Law (DIGinLaw); University of Osijek - Faculty of Law Osijek;
Creative Commons license CC BY-NC-SA 4.0.

ISBN 979-12-5510-276-2 (PDF)
ISBN 979-12-5510-278-6 (EPUB)
DOI 10.54103/milanoup.215