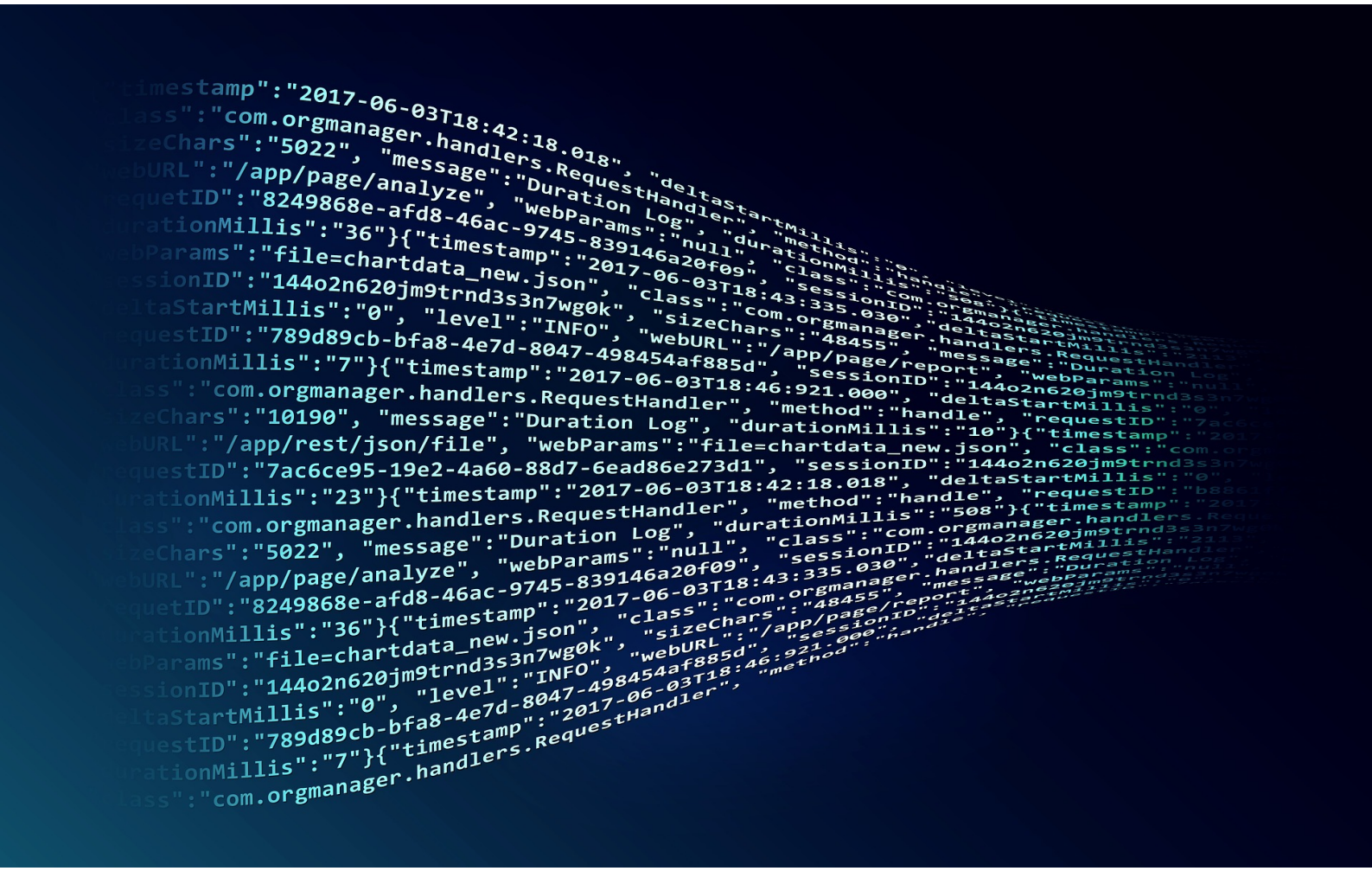
ISSN 2384-9169
NUMERO SPECIALE
www.eurojus.it

Big data and Public Law: new challenges beyond data protection



UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI DIRITTO PUBBLICO ITALIANO E SOVRANAZIONALE
Centro di Eccellenza Jean Monnet
Via Festa del Perdono, 7 - 20122 Milano - Italia/Italy

Co-funded by the Erasmus+ Programme of the European Union

UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI DIRITTO PUBBLICO
ITALIANO E SOVRANAZIONALE

Centro di Eccellenza Jean Monnet
Via Festa del Perdono, 7 - 20122 Milano - Italia/Italy

This special issue is published with the contribution of the Università degli Studi di Milano within the initiatives of the Jean Monnet Center of Excellence, coordinated by Prof. Francesco Rossi Dal Pozzo, which is funded by the European Commission and dedicated to the "Digital Single Market and Cyber Security ". All the Centre of Excellence's initiatives are also hosted on the centrojeanmonnet.eurojus.it website.

Diana-Urania Galetta[(*)]

Introduction to the papers of the first Edition of the Doctoral Seminar in Public, International and European Union Law of the University of Milan, "*Big Data and Public Law: new challenges beyond data protection*".

This special issue of *EuroJus* collects the papers presented during the first edition of the seminars of the Doctorate in Public, International and European Law of the University of Milan that took place between the 15th and the 17th of October, 2018 in the prestigious setting of Palazzo Feltrinelli, on the shores of the lake in Gargnano sul Garda.

Papers' collection as well at the editorial revision of the papers were carried out solely by *Gherardo Carullo*, Research Assistant at the University of Milan, whom I'm especially grateful to also for the precious help in organizing the two days of seminar in Gargnano.

Participants were selected with an open call for PhD students and recent post-docs, titled "Big Data and Public Law: new challenges beyond data protection". The aim was to gather papers that could, in various ways, identify the challenges deriving from the increasing digitization of society and its actors, in particular by examining how the most recent technologies can influence national and supranational law.

Therefore, the criteria used by the selection Committee of full Professors of the University of Milan favoured those paper with the most interdisciplinary approach, encompassing international law, constitutional law, tax law and administrative law; and to this end, the call identified three main subject areas, which corresponded to the three different panels.

The introduction to the seminar was delivered by *Jean-Bernard Auby*, distinguished Professor of Public Law at Sciences-Po (Paris, France) who held a *lectio magistralis* which provided a wide and inspiring overview of the various issues that lawyers face due to the digital revolution, both at the local level, and globally.

The first panel – chaired by myself, in my capacity as Director of the PhD Programme in Public, International and EU Law of the University of Milan and as organizer of the doctoral seminar, and with the final remarks of *Giuseppe Marino*, Tax Law Professor at the University of Milan – titled "Big Data and Public Law: artificial intelligence, algorithmic decision and algorithmic transparency, Big Data and Taxation", and focused on the role of technology in relation to human rights.

The first paper of this panel, of *Mauri*, addresses the delicate issue of the use of artificial intelligence for military purposes. In particular, the article analyses the admissibility

(*)[(*)] Director of the PhD Programme in Public, International and EU Law of the University of Milan. Full Professor of Administrative Law and European Administrative Law.

of so-called Algorithmic Target Construction (ATC), in order to assess the legality of such instruments in relation to human rights.

The second paper, of *Dal Monte*, focuses on human rights, as well; its special focus is on whether, and to what extent, the use of big data can constitute a risk for the individual's self-determination and for the implementation of his/her fundamental rights. After an introduction on the notion of human dignity, the text unfolds through a comparative law analysis between Europe and the United States, thus evaluating how competition rules and antitrust powers of the public authorities can be used as a tool to protect (also) the rights of the individual.

On the tax law side, *Sut*'s paper analyses the challenges that increasing digitalization of the internal market poses for Member States and for European institutions. After a brief exposition of the new problems that the digital market poses under a tax law perspective, the author proposes an interesting analysis of the recent proposal for a Council Directive on the Common System of Digital Services.

To conclude the first panel, *Pitto*'s paper focuses on another very topical issue, namely electoral freedom and the use of big data as a tool for the dissemination of political messages. The actuality of the problem, and the enormous size of it, is approached through an interesting historical analysis, starting from the traditional means of political propaganda. The author stresses out what has actually changed with the new tools offered by Information and Communication Technologies (ICT); and, in particular, how the use of big data to convey messages on social media might have changed, or not, the traditional relationship between voters and their representatives.

The second panel – chaired by *Daniele Senzani*, Professor of Public Law at the University of Bologna, and with the final remarks of *Gabriele Della Morte*, Professor of International Law at the University of Milan-Cattolica – titled "Big Data and State Jurisdiction (The un-territoriality of Data): how centrality of territoriality is challenged by the present day dynamics governing the search and seizure of digitized information", and focuses on problems arising from the immateriality of digital assets, as well as the speed with which data move, and can be moved, from one nation to another.

Cantekin's paper addresses specifically the problem of cross-border data transfers. The author begins by analyzing the case US v. Microsoft, and then the US Cloud Act. Based on these premises, the article focuses on the analysis of the opposing interests inherent in data management, the protection of individuals and free trade.

The second contribution to the panel, by *Piovesani*, focuses on data protection litigation. The author analyzes in particular Regulation 2016/679/EU, the General Regulation on Data Protection (so-called GDPR), and Regulation 2012/1215/EU, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (so-called B1R). The author deals in particular with the problems related to the coordination of proceedings before different courts or tribunals, analyzing the discipline referred to in the GDPR and how it can be interpreted in light of the rules provided by B1R.

Regarding criminal trials, *Bartoli* analyzes the problem of accessing data in criminal proceedings. In particular, the author focuses on the problems posed by the fact that data is now often kept in the hands of private companies (so called cloud); so that access to the physical facilities where such data is stored (data centers) can sometimes be extremely complex, if not impossible, due to territorial limitations and/or jurisdiction limitations.

The paper by *Jolly* focuses on criminal trial and analyzes the issues raised by the development of distributed register technologies (so-called blockchain). From a criminal law point of view, the author assesses in particular what effects the new delocalized and decentralized tools based on blockchain have on national jurisdiction. The paper thus evaluates how the targeted public theory could be referred to in order to establish jurisdiction over offences enabled or facilitated by the use of such technologies.

Lastly, the third panel – chaired by *Russel L. Weaver*, Professor at the University of Louisville, Louis D. Brandeis School of Law (Kentucky - USA) and with the closing remarks of *Jean-Bernard Auby* and myself – titled "Digitization of Public Administration and Big Data: tools, challenges and prospects of the transition to a digitalized public administration", and focuses on the transformations underway in the public administration, both as regards the modalities of action, and the protection and promotion of individual rights and freedoms.

The first paper of the panel, by *Pinotti*, analyses a problem at the basis of digitization, i.e. access to the source code of software used by public administrations. Thanks to the analysis of the recent case-law on this matter, the author verifies to what extent the right of access can be deemed to exist in relation to the source code of a software licensed to a public administration, when such software has been used to adopt an administrative decision.

Schneider's second paper of the panel questions what limitations can be said to exist with respect to the use of intelligent algorithms, and therefore of artificial intelligence, for the adoption of administrative decisions. The author underlines how crucial it is to be able to guarantee transparency and accountability in public decisions. For this reason, the paper calls into question the use of artificial intelligence by public administrations, especially in those circumstances where the software does not allow to comprehend the reasons for a given output.

Alberti' s paper also focuses on the topic of the use of artificial intelligence by public administrations. However, unlike Schneider, he assesses the compatibility of AI with the due process principle. In particular, the author analyzes how the use of data can allow a deeper knowledge by public administrations and, therefore, how the decision-making process can change for the better thanks to the use of artificial intelligence.

Finally, *Lima De Arruda* introduces with her paper the concrete example of the state of digitalization of the public administration in Brazil. In this context, the author explains how the use of information and communication technologies can have disruptive effects for the Brazilian bureaucracy, from tax authorities to the health system.

1st Edition of the Seminars of the PhD School in Public, International and European Union law of "Università degli Studi di Milano"

15-17 October 2018, Palazzo Feltrinelli, piazza Vittorio Veneto, Gargnano sul Garda

Big data and Public Law: new challenges beyond data protection

October 16, 2018

Panel I - Big Data and Public Law: artificial intelligence, algorithmic decision and algorithmic transparency, Big data and Public Health, Big data and Taxation

I.1 DIEGO MAURI - "Algorithmic Target Construction" and the Challenges by International Human Rights Law
I.2 FIORELLA DAL MONTE - The use of big data as a risk for individual self-determination and the implementation of competition law in the digital market - A comparative approach between the European Union and the United States of America
I.3 SILVIA SUT - Taxation and Big data: an analysis of the proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services (Proposal of the European Commission COM (2018)
I.4 SIMONE PITTO - Electoral freedom in the age of big data: an historical critique

Panel II - Big Data and State Jurisdiction (the un-territoriality of data): how centrality of territoriality is challenged by the present-day dynamics governing the search and seizure of digitized information

II.1 ENNIO PIOVESANI - The interface between the jurisdictional rules of Reg. (EU) No 2016/679 and those of Reg. (EU) No 1215/2012
II.2 KAYAHAN CANTEKIN - Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?
II.3 LAURA BARTOLI - Digital evidence for the criminal trial: limitless cloud and state boundaries
II.4 LOREN JOLLY - Towards an alternative to territorial jurisdiction to face criminality committed through or facilitated by the use of blockchains

October 17, 2018

Panel III - Digitization of Public Administration and Big Data: tools, challenges and prospects of the transition to a digitalized public administration

III.1 GIULIA PINOTTI - Automated administrative procedure and right of access to source code
III.2 GIULIA SCHNEIDER - The Algorithmic Governance of Administrative Decision-Making: Towards an Integrated European Framework for Public Accountability
III.3 ISABELLA ALBERTI - Artificial Intelligence in the public sector: opportunities and challenges
III.4 CARMEN SILVIA LIMA DE ARRUDA Government discretion in digitizing public administration – the Brazilian perspective

Panel I - Big Data and Public Law: artificial intelligence,algorithmic decision and algorithmic transparency, Big data and Public Health, Big data and Taxation

I.1

"Algorithmic Target Construction" and the Challenges by International Human Rights Law

SUMMARY**:** 1. Introduction. – 2. Algorithmic Target Construction (ATC) – 3. ATC under IHRL. – 3.1. Data Collection. – 3.2. "Categorical" Decisions. – 3.3. "Legibility". – 3.4. Subjection to Solely-Automated Decisions. – 4. Conclusion: Is A Different Approach Possible?

1. The first use of an armed drone allegedly occurred during the US hunting of Osama bin Laden, and more precisely on February 4, 2002, when the CIA spotted a «tall man», much resembling bin Laden, around whom several people were «acting with reverence», and fired an *Hellfire* missile against him.[1] The CIA operators' assumption turned however to be untrue, as the target was later discovered to be a local unfortunately – for him – the same height as bin Laden. Interestingly enough, US authorities insisted the target was «legitimate»; the Pentagon then-spokeswoman so declared: «We're convinced that it was an appropriate target … [but] we *do not know yet exactly who it was*».[2]

Here the essence of a "signature strike" is captured perfectly. The term – now one of the art – refers to a methodology for selecting actual targets for drone strikes basing solely on their observed pattern of behavior (i.e. their "signature").[3] The target's personal identity remains unknown *before* the strike and may remain so also *after* it. It differs from a "personality strike" in that in the latter the target's personal identity is known to the authorities before the strike, which as a matter of fact takes place by virtue of the target's personal identification. Signature strikes have gained momentum under the Obama Administration, albeit some initial reservations.[4] They are believed to avoid a «huge number of civilian casualties»,[5] and to work as an appropriate tool to address the challenges of the well-known Global War on Terror.[6]

1 The episode is told by R. SIFTON, *A Brief History of Drones*, in *The Nation*, 27 February 2012, available at: http://www.thenation.com/article/166124/brief-history-drones#.

2 *Ibidem*, italics mine.

3 For a definition of signature strikes, reference can be made to K. BENSON, *"Kill 'em and Sort it Out Later:" Signature Drone Strikes and International Humanitarian Law*, in *Global Business & Development Law Journal*, 2014, p. 18. See also S. HOLEWINSKI, *Just Trust Us*, in P. BERGEN, D. ROTHENBERG, *Drone Wars. Transforming Conflict, Law, and Policy*, Cambridge, 2014, p. 45-46; K. KINDERVATER, *The Emergence of Lethal Surveillance: Watching and Killing in the History of Drone Technology*, in *Security Dialogue*, 2016, p. 224 ff.; T. WALL, T. MONAHAN, *Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes*, in *Theoretical Criminology*, 2011, p. 239–245.

4 See the anecdote narrated by M. ZENKO, *Targeted Killing and Signature Strikes*, in *Council On Foreign Relations*, 16 July 2012, available at: http://blogs.cfr.org/zenko/2012/07/16/targeted-killings-and-signature-strikes/ (citing one legal advisor that so described the President's unease at striking at military-age males associated with terrorist activities but whose personal identity remained unknown: «[H]e didn't like the idea of kill 'em and sort it out later»).

5 See the Report *Emerging from the Shadows: US Covert Drone Strikes in 2012*, in *Bureau Of Investigative Journalism*, 3 January 2013, available at: http://www.thebureauinvestigates.com/2013/01/03/emerging-from- the-shadows-us-covert-drone-strikes-in-2012-2/.

6 Numbers and figures regarding the first year of the Trump Administration confirm that drone strikes are the first choice in counterterrorism abroad. See https://www.thebureauinvestigates.com/stories/2018-01-19/strikes-in-somalia-and-yemen-triple-in-trumps-first-year-in-office (showing that the number of strikes conducted in Yemen and Somalia in 2017 is nearly more than triple the number relating to the precedent year).

The gist of signature strikes is that they rely essentially on a process that can be named "Algorithmic Target Construction" (ATC). Current drone technology requires a human decision-maker to be present at the act of engaging that target; the ultimate decision about the life or death of the individual is thus entrusted to a human agent. The development and deployment of Lethal Autonomous Weapons Systems (henceforth: LAWS) puts such model in discussion as not only target selection, but also target engagement will be entrusted to a non-human decision-maker.[7]

The advent of LAWS is likely to act as a veritable turning point in our understanding of using force against humans; several features of this technology, and the impact thereof on international law, have already been tackled.[8] The present contribution aims at assessing the impact ATC may have on human rights. In Section 2 a brief description of how ATC functions will be provided; most suggestions will be drawn from current uses of technology in performing signature strikes via armed drones. In Section 3 I will then turn to the framework of international human rights law (IHRL) with a view to showing that ATC is suitable to affect basic human rights. I will then draw conclusions leaving some radical questions open (Section 4).

2. ATC can be defined as a process allowing for target selection and engagement through algorithms.[9] This concept has been recently adopted in a Briefing of the Geneva Academy of International Humanitarian Law and Human Rights.[10] Proceeding in reverse order, "Construction" refers to a methodology of gathering and then re-elaborating **data** which constitute the very input of the process. The outcome is the identification of a "Target", namely an individual or group of individuals that will be made the object of force delivery, while the process through which data are re-elaborated is "Algorithmic". The notion of ATC can be "unpacked" so as to distinguish between two particularly salient temporal stages at least, namely data collection and later decision-making.

As far as data collection is concerned, it is generally considered as the first component of "processing". To be employed in an operational scenario (such as battlefield or a law-enforcement operation), LAWS will need to gather as much data as possible from the field, and therefore they will presumably be endowed with software for carrying out a preliminary screening of individuals and places.[11] Collected data will then go through a process of organization and structuring; in particular, applying the same methodology currently in use for signature strikes, LAWS will likely

7 See among others: *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns*, UN General Assembly, A/HRC/23/47 (9 April 2013); *Losing Humanity: The Case Against Killer Robots*, Human Rights Watch (November 2012). The forum that is currently hosting discussion on «emerging technologies in the area of [LAWS]» is the Assembly of the States Party to the 1980 Convention on Certain Conventional Weapons (hereinafter: CCW), which decided to convene three Meetings of Experts between 2014 and 2016; the 2016 Fifth Review Conference of the CCW then established a Group of Governmental Experts (GGE) that held its meeting on November 2017, April 2018 and August 2018. A new round of meetings will probably take place in 2019. See *amplius* https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument.

8 For a recent and thorough analysis, see D. AMOROSO, *Jus in bello and jus ad bellum arguments against autonomy in weapons systems: A re-appraisal*, in *QIL Zoom-In*, 2017, p. 5-31.

9 For a better understanding of how algorithms work and how influential their use can get, see P. ZELLINI, *La dittatura del calcolo*, Milan, 2018.

10 See M. BREHM, *Defending The Boundary. Constraints And Requirements On The Use Of Autonomous Weapon Systems Under International Humanitarian And Human Rights Law*, in *Academy Briefing No. 9*, May 2017, available at: https://www.geneva-academy.ch/joomlatools-files/docman-files/Briefing9_interactif.pdf.

employ software allowing for detecting individuals or group of individuals possessing certain personal attributes that are considered as statistically correlated to certain conducts – a process commonly referred to as "profiling".[12] The purpose of such process is to *predict* an individual's action on the basis of a so-called "pattern of life analysis"; the individuals whose data are gathered and elaborated by the machine are therefore "reduced" to a profile and put into "categories". Such type of analysis and technique of re-elaboration of personal data has been used for signature strikes since the beginning,[13] so that LAWS will be programmed so is more than a mere prevision.[14] In short, «an individual's pattern of behavior – or "signature" – serves as a proxy for determining if that individual» may be a target for the use of force.[15] In terms of technological feasibility, suffice it to recall that recently IBM has declared that it was about to offer an algorithm capable of distinguishing terrorists out of refugees.[16] As has been conveniently pointed out, «one of the most acute dangers of profiling is the fact that it tends to reduce the person to the profile generated by automated processes which are *liable to be used as a basis for decision-making*».[17]

Decision-making is another crucial step of ATC. While the current practice of signature strikes leaves the final decision (i.e. whether to engage or not the selected target) to a human operator, automated decision-making (understood as a process where taking the final decision is entrusted to a software, i.e. to a non-human operator) is already in place in different contexts, such

11 See A. SPAGNOLO, *Human rights implications of autonomous weapon systems in domestic law enforcement: sci-fi reflections on a lo-fi reality,* in *QIL Zoom-in*, 2017, p. 43.

12 See *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; hereinafter: GDPR), art. 4(4): «"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».

13 N. ABÈ, *Dreams in Infrared: The Woes of an American Drone Operator*, in *Spiegel Online*, 14 December 2012, available at: http://www.spiegel.de/international/world/pain-continues-after-war-for-american-drone-pilot-a-872726.html («[w]e watch people for months. We see them playing with their dogs or doing their laundry. We know their patterns like we know our neighbors' patterns. We even go to their funerals»); G. MILLER, *At CIA, a Convert to Islam Leads the Terrorism Hunt*, in *Washington Post*, 24 March 2012, available at: http://articles.washingtonpost.com/2012-03-24/world/35447818_1_cia-officials-robert-grenier-ctc.

14 See M. SCHMITT, J. S. THURNER, *"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, in *Harvard National Security Journal*, 2013, p. 268.

15 Paraphrasing BENSON, *Kill 'em and Sort It Out Later*, cit., p. 29.

16 P. TUCKER, *Refugee or Terrorist? IBM Thinks Its Software Has the Answer*, in *Defense One*, 27 January 2016, available at: http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-has-answer/125484/.

17 See the Report of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Application of Convention 108 to the Profiling Mechanism: Some Ideas for the Future Work of the Consultative Committee*, 11 January 2008, p. 5-6, available at https://rm.coe.int/16806840b9, italics mine. The matter is of particular concern when it comes to policing algorithms that may subject minorities to greater surveillance and therefore police force; see K. K. KOSS, *Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post*-Wardlow *World*, in *Chicago-Kent Law Review*, 2015, p. 301-334.

as recruitment, behavioral advertisement, access to credit.[18] It has been argued that entrusting LAWS to take engagement decisions will be more efficient than having a human operator do so.[19]

As will be illustrated in the following, it is by reason of dangers associated with the algorithmic processing of such data (to name a few, poor final decisions, misjudgments, or an alarming inclination for discriminatory outcomes) that a certain degree of human control over automated decision-making has been retained of paramount importance. It is however questionable the extent to which human will be able to exert control on such processes, especially when machine-learning or self-learning algorithms are employed.[20] Brief, LAWS employing machine-learning algorithms in ATC will be able to generate their own rules and conduct basing on their initial databank and gained experience "in the field",[21] which means that their ability to select and engage targets properly will depend on previous experience in the relevant operational field (battlefield; law-enforcement area of operations; etc.).[22] This has an impact on what will be later defined as "legibility" of the system: human operators will hardly be in the condition to understand how and why a LAWS operating through self-learning algorithms acted in a certain way.

In sum, ATC will be a key feature in the development of next-generation LAWS. As a complex process, it will involve data gathering, data elaboration and more importantly automated decision-making allegedly independent of human intervention. For all these steps, human rights of the potential targets are put at stake to some extent, which implies that in building algorithms developers must take those rights in due consideration – «seriously», in the famous words of Ronald Dworkin.

3. In order to assess the impact the development of ATC can have on IHRL, it seems appropriate to enucleate at least four critical features of that process: (1) mass surveillance techniques; (2) "profiling" or "categorization" of potential targets; (3) "legibility" of the algorithms leading to the final decision; (4) absence of human control on the decision-making process. For each feature a short recapitulation of existing case-law and scholarship is provided, with a view to

18 Algorithms that rely on "profiling" of the concerned individuals to reach a "decision" are currently employed, for example, to refuse an online credit application or e-recruitment practice; see GDPR, Recital 71, and G. MALGIERI, G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 253. For an interesting overview of today's pervasiveness of profiling and automated decision-making, see F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge-London, 2015, and A. CHANDER, *The Racist Algorithm?*, in *Michigan Law Review*, 2017, p. 1023-1045.

19 For instance, human operators are often exposed to "machine-bias". See T. CHENGETA, *Defining the emerging notion of "Meaningful Human Control" in Weapon Systems*, in *New York University International Law and Politics*, 2017, p. 852-853.

20 For a definition of "machine-learning", see S. SHALEV-SHWARTZ, S. BEN-DAVID, *Understand Machine Learning. From Theory to Algorithms*, Cambridge, 2014.

21 See O. ULGEN, *Kantian Ethics in the Age of Artificial Intelligence and Robotics*, in *QIL Zoom-In*, 2017, p. 73.

22 See ICRC, *Report of the ICRC Expert Meeting, Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*, 9 May 2014, available at: https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014; id., *Report of the ICRC Expert Meeting, Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, 15-16 March 2016, available at: https://www.icrc.org/en/publication/4283-autonomous-weapons-systems.

exploring whether similar rules apply – *mutatis mutandis* – when it is mainly the right to life to be at stake.

3.1. Widespread practices of blanket interception of communications and mass collection of data raise growing concern among human rights bodies as far as the right to privacy is concerned.[23] While the right to privacy is notoriously subject to restrictions,[24] strict conditions apply when it comes to public authorities putting in place massive surveillance and the systematic collection and storing of data.[25] A wide spectrum of data is likely to be gathered for the purposes of ATC. Generally speaking, "data" that are relevant under the right to privacy encompass "personal",[26] "sensitive",[27] "biometric"[28] and "big" data.[29] While in the recent decades there has been a growing concern about the need to protect these data, undeniably States still enjoy a certain room for maneuver.

Possibly thanks to the pervasiveness of new technologies of data interception and re-elaboration, however, human rights bodies have raised the bar for such operations to be conducted lawfully. For instance, the ECtHR has scrutinized practices such as the interception of private

23 To catch a glimpse of the existing discourse around these practices, see UNGA Res. 68/167, 21 January 2014, available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167; see also OHCHR, *The Right to Privacy in the Digital Age*, Report of 30 June 2014, UN doc A/HRC/27/37, available at: http://undocs.org/A/HRC/27/37. On the right to privacy generally, see Art. 12 UDHR («No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks»); see Art. 17 ICCPR and *General Comment No. 16, Article 17*, 8 April 1988; Art. 8 ECHR. For an historical overview of the international provisions protecting the right to privacy, see G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti*, Naples, 2018, p. 75 ff..

24 See *General Comment No. 16*, cit., § 7 («[a]s all persons live in society, the protection of privacy is *necessarily* relative», italics added); Art. 8(2) ECHR (listing three parameters for limiting the right to privacy, namely legality, necessity and proportionality).

25 Such considerations move from the assumption that massive storage of data as well as constant surveillance are dangerous for a democratic society. Yet decades ago the European Court of Human Rights (hereinafter: ECtHR) acknowledged that «an unlimited discretion to subject persons within their jurisdiction to secret surveillance» would risk «undermining or even destroying democracy on the ground of defending it»; see ECtHR, *Klass et al. v. Germany*, No. 5029/71, judgment (plenary), 6 September 1978, § 49. For a discussion on the right to privacy as at particularly at stake when counterterrorism measures are put in place, see *amplius* M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Naples, 2012.

26 Defined as «any information relating to an identified or identifiable» individual (see GDPR, art. 4(1)). See also the *Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, adopted by the 128th Session of the Committee of Ministers in Elsinore, Denmark, on 18 May 2018, CM/Inf(2018)15-final (CETS No. 108) (hereinafter: Modernized Convention), art. 2.

27 For a list of personal data that must be considered as «sensitive» inasmuch as revealing certain personal characteristics, see GDPR, art. 9.

28 «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, such as facial images or dactyloscopic data» (GDPR, art. 4(14)).

29 It is impossible to account for the immense literature that has been developed on big data so far. See DELLA MORTE, *Big Data*, cit., p. 159-169, with references.

communications[30] and addressed the issue of technologies that allow for the monitoring of private activities by State authorities. In the *Szabó and Vissy* case the Court held that while that «governments resort to cutting-edge technologies» is «a natural consequence of the forms taken by present-day terrorism», it would «defy the purpose of government efforts to keep terrorism at bay … if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives».[31] It follows that legal safeguards have to be put in place by States when employing such «strategic, large-scale interception» of personal data.[32] What should be taken note of is that in assessing the respondent State's safeguards the Court interpreted the requirement of necessity «in a democratic society» provided for by Art. 8(2) ECHR as requiring the more stringent «strict necessity» *by reason of* the pervasiveness of the cutting-edge surveillance technologies based on «automated and systemic data collection».[33] In short, the rationale the Court leans on seems to be the following: *the more impactful on human rights a surveillance measure is, the more stringent the conditions for the resort thereto need to be*.

In the case of LAWS, the purpose of data collection would be *inter alia* to identify a target for the use of force. In this sense, it would be the right to life – the supreme one, an absolute one and one from which no derogation is allowed – to be put primarily at stake. It follows that requirements for gathering such personal data need to be far more stringent than in other contexts that have come under the scrutiny of human rights bodies so far. A blanket, massive collection of personal data for law-enforcement purposes would virtually expose every individual, in a given geographical area, to a violation of their right to privacy.

3.2. Turning to the decision-making process, human rights bodies have so far voiced concern regarding decisions taken by public authorities on the basis of an automated processing of personal data. In particular, algorithmic processes may put individuals under "categorical" suspicion solely due to their membership – either alleged or effective – in a certain category.

For instance, arresting an individual on the basis that his/her affiliation to an organization is indicative of an higher propensity of committing illegal acts has been considered by the Court of Strasburg as a violation of Art. 5 ECHR.[34] Such practice has important implications on the right to equality and non-discrimination as well.[35] It has been repeatedly outlined how profiling tends to

30 See *Liberty et al. v. the United Kingdom*, judgment, 1 July 2008; *Kennedy v. the United Kingdom*, judgment, 18 May 2010, and more recently *Roman Zakharov v. Russia* [GC], No. 47143/06, judgment, 4 December 2015.

31 See *Szabó and Vissy v. Hungary*, No. 37138/14, judgment, 12 January 2016, §§ 67, 68.

32 *Ibidem*, § 67.

33 Ibidem, § 73 *in principio* and 67.

34 See *Shimovolos v. Russia*, No. 30194/09, judgment, 21 June 2011 (for a case regarding an individual being subject to a deprivation of his personal liberty as his name had been included in a «surveillance database» set up by Russian authorities that employed algorithmic processes to detect «potential extremists»). See also *Ostendorf v. Germany*, No. 15598/08, judgment, 7 March 2013 (for a case regarding a deprivation of personal liberty considered lawful also by virtue of the fact that public authorities had not based their determination on the individual being enlisted in a police database).

35 For a general appraisal of the principle of non-discrimination, see HRCttee, *General Comment No. 18: Non-Discrimination*, 10 November 1989, § 12; see also *Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination*, UN doc A/HRC/29/46, § 22.

expose individuals to negative forms of discrimination, especially based on racial and ethnic origin, religious or other beliefs and political opinions, just to name a few.[36]

The decisive element in assessing the lawfulness of automated decision-making appears to lie in that such process fails to consider the individual *as such*; rather s/he is considered only as belonging to an abstract category. Failure in appreciating the actual situation of an individual is problematic in human rights bodies' recent case-law. Decisions regarding passports withdrawal or imposition of travel bans have been considered as in violation of human rights because public authorities have not been able to carry out a *fresh review* of the individual situation, thus imposing restrictions that could not be characterized as «necessary in a democratic society».[37] In a Dissenting Opinion delivered by three judges of the Court of Strasburg, the categorical treatment of people who happened to be at a certain place in a certain hour – without distinguishing between demonstrators and bystanders – by police forces was deemed in contrast with the right to liberty in that individuals had been treated «*like objects*».[38] Again, the rationale that underlies these judgments is that *each and every decision affecting human rights at a certain degree need to take an individual situation into due account*.

Applying this rationale to LAWS, it has been already outlined that their unique feature lies in that not only data collection and elaboration, but also the final decision – delivering lethal force against an individual – are entrusted to a non-human agent. In order for ATC to be consistent with the prohibition on categorization, it therefore has to be developed in a way that ensures that the *specific* features of each and every situation are taken in due account by LAWS before resorting to force. On closer inspection, such conclusion is implied in the well-known requirements for the use of force that IHRL instruments establish with respect to the right to life: «absolute necessity» and «proportionality».[39] A lethal decision resulting solely from a pattern-of-life analysis is inconsistent with the right to life, as implied by the abovementioned case-law: if life can be taken only when «absolutely necessary», and if arguably decisions taken upon individual categorization are incompatible with the – less stringent – requirement of «necessity in a democratic society», then *a fortiori* a categorical killing as such would be at odds with the right to life.[40] Incidentally, what has

36 See *amplius* Brehm, *Defending the boundaries*, cit., p. 61.

37 See ECtHR, *Battista v. Italy*, No. 43789/09, judgment, 2 December 2014; *Stamose v. Bulgaria*, No. 29713/05, judgment, 27 November 2012 (for cases concerning the freedom of movement as enshrined by Art. 2 Prot. 4 ECHR); *contra*, see *Landvreugd v. the Netherlands*, No. 37331/97, judgment, 4 June 2002, particularly at § 70.

38 See ECtHR, *Austin and Others v. the United Kingdom* [GC], judgment, 15 March 2012, Joint Dissenting Opinion by Judges Tulkens, Spielmann and Garlicki, particularly at § 10.

39 See Art. 2(2) ECHR; Art. 6(1) ICCPR; Art. 4(1) ACHR; Art. 4 ACHPR. For relevant case-law, see *ex multis* ECtHR, *Giuliani and Gaggio vs. Italy*, No. 23458/02, 24 March 2011, § 176 (affirming that «a stricter and more compelling test of necessity must be employed than that normally applicable when determining State action is "necessary in a democratic society" under paragraph 2 of Articles 8 and 11 of the Convention»); HRCttee, *Suarez de Guerrero v Colombia*, Views, Comm no R.11/45, 9 April 1981, Supp No. 40 (A/37/40) at 137 (1982); IACtHR, *Nadege Dorzema et al v Dominican Republic*, judgment (Merits, Reparations and Costs), 24 October 2012.

40 See ECtHR [GC], *Streletz, Kessler and Krenz v. Germany*, Nos. 34044/96, 35532/97 and 44801/98, judgment, 22 March 2001, § 73 (in which consideration was given to «recourse to anti-personnel mines and automatic-fire systems, in view of their automatic and indiscriminate effect, and the categorical nature of the border guards' orders to "annihilate border violators … and protect the border at all costs"»).

been said so far might work as a principled argument against signature strikes in today's drone operations.

However, what current case-law attaches great importance to the absence of a fresh review on an individual situation (an *objective* element) as such rather than to the subject tasked with carrying out such review (a *subjective* element). Restating the point, it does not stem from the foregoing that LAWS employing "categorical", but situationally appropriate, decisions would be proscribed, even if in the decision-making process human deliberation is absent.

3.3. Another issue regarding automated decision-making is that individuals affected by such process may not know how and why algorithms have led to the final decision. It does not seem necessary to underscore how pressing the issue gets when it comes to decisions particularly suitable for affecting basic human rights, such as the right to life.

To begin with, current IHRL applicable to the right to privacy acknowledges the individual's right to *understand* the functioning and the impact of algorithms concerning him/her. For instance, this right is inferable from several provisions regarding data protection adopted in the frameworks of the Council of Europe[41] and the European Union[42], in both cases in binding terms. In particular, the right to know the reasons that underlie an automated decision derives from a set of several rights such as the right to receive *ex ante* information from data controllers and the right to access to information *ex post*, that is after the decision-making process has been undertaken or concluded.[43] In the GDPR's words, the individual has a right to be informed about/be given access to «*meaningful* information about the logic involved, as well as the *significance* and the *envisaged consequences* of such processing» for the individual. Some have proposed to interpret the right as encompassing a right to *legibility*, in the sense that algorithms must be designed and built in a way that they are both transparent and comprehensible to people concerned thereby.[44] Legibility therefore finds a ground of justification in that it is intended to ensure that *automated decision-making does not turn into an unintelligible process*.

Thinking of ATC in terms of legibility turns to be particularly effective through the lens of the right to life as well, for the following reasons. First, an ex-ante knowledge of how algorithms involved in the ATC process appears to satisfy the legal requirement of legality of the use of force as enshrined in IHRL: any deprivation of life must result from the exercise of a power that is provided either in domestic law or in international law, or both.[45] Arguably the protection of the right to life necessitates «an appropriate legal and administrative framework *defining the limited*

41 See the Modernized Convention, art. 9; *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CM(2018)2-addfinal (CETS No. 223) (hereinafter: Explanatory Report), §§ 71-83.

42 See GDPR, arts. 13, 14 (right to notification), 15 (right to access) and art. 22 (right not to be subject to a decision based solely on automated processing, including profiling). For the sake of clarity, references to the GDPR are intended only to draw analogies and not to suggest that it is applicable to our subject matter: Art. 2.2.d clearly excludes such chance.

43 See for instance GDPR arts. 13(2)(f), 14(2)(g) and 15.

44 See in particular MALGIERI, COMANDÈ, *Why a Right to Legibility*, cit., p 245.

45 Art. 6(1) ICCPR, Art. 2(1) ECHR, and Art. 4(1) ACHR all require expressly a legal basis, whereas the ACtHPR does not.

circumstances in which law enforcement officials may use force and firearms, in the light of the relevant international standards».[46] If such regulatory framework is obscure, or fails to provide individuals with understandable – "legible" – indications about the conditions in which LAWS resort to lethal force in law-enforcement situations (the abovementioned «limited circumstances»), the requirement of legality will be hardly met. The issue gets all the more troublesome once the scenario is taken into consideration where ATC employ self-learning algorithms, which as explained in the foregoing ensure low rates of predictability.

Second, ex-post explanation about the process that has actually led to a specific automated decision comes to the fore from the perspective of procedural obligations under IHRL. Procedural obligations are a particular form of positive obligations involving the duty to invest into (alleged) violations of a right and to prosecute those who are responsible; in this sense, it is «not an obligation of result but of means only».[47] In order for an investigation to comply with human rights standards, it allegedly has to be *capable* of leading to a determination of whether the force used was justified *in the circumstances*.[48] In the dynamic of ATC processing, it is therefore of paramount importance that public authorities provide an intelligible account of how an automated process has worked; a failure to "explain how",[49] *reddere rationem*, may lead to responsibility under IHRL.[50] With respect to the use of force, if LAWS employ an ATC technique that does not allow their users to understand how and why the machine has taken that particular decision – which may be the case, again, when self-learning algorithms are employed –, it follows that the right to life would be violated under the procedural tenet as well.[51]

To sum, the right to legibility as pushed forward by scholarship is a useful tool for testing the compatibility of ATC with IHRL also with respect the right to life. Failure to provide information and explanation about how and why algorithms work and lead to a certain decision,

46 See ECtHR, *Giuliani and Gaggio v. Italy*, No. 23458/02, judgment, 24 March 2011, § 209.

47 See ECtHR [GC], *Šilih v. Slovenia*, § 193. See also IACtHR, *Cantoral Huamaní and Garcia Santa Cruz v. Peru*, Preliminary objection, merits, reparations and costs, 10 July 2007, Series C 167 (2007), § 131, and *Pueblo Bello Massacre v Colombia*, 31 January 2006, Series C 140 (2006), § 143. Its aims are: (i) ensuring that those responsible are brought to justice; (ii) promoting accountability and preventing impunity; (iii) avoiding denial of justice; (iv) eventually drawing necessary lessons for revising practices and policies with a view to avoiding repeated violations.

48 ECtHR, *Isayeva v. Russia*, No. 57950/00, judgment, 24 February 2005, §§ 221-223 (for a case where the ineffectiveness of the investigation was predicated in that it had made «few attempts to find an explanation for … serious and credible allegations», thus placing the need for an explanation about the use of force at the center of the right to life under its procedural tenet).

49 See ECtHR, *Khodorkovskiy and Lebedev v. Russia*, No. 11082/06 and 13772/05, judgment, 25 July 2013, § 848 (discussing the algorithmic method used for distributing convicted individuals among prisons).

50 The issue has also been tackled from the standpoint of international humanitarian law. See P. MARGULIES, *Making Autonomous Weapons Accountable: Command Responsibility for Computer-Guided Lethal Force in Armed Conflicts*, in J. OHLIN (ed), *Research Handbook on Remote Warfare*, Cheltenham-Northampton, 2017, p. 23 (underscoring that the onus is on the State to provide adequate details about decision-making processes at large).

51 Some scholars that support the development and deployment of LAWS are apparently prone to accepting the idea that human operators may not be able to understand how and why LAWS take specific lethal decisions. See for instance K. ANDERSON, D. REISNER, M. WAXMAN, *Adapting the Law of Armed Conflict to Autonomous Weapons Systems*, in *International Law Studies*, 2014, p. 394 (arguing that «as machine-learning and artificial intelligence technologies develop, it is becoming increasingly clear that human beings may not necessarily always be able to understand how (and possibly why) autonomous systems make decisions»).

both *ex ante* and *ex post*, will expose public authorities employing LAWS to responsibility under IHRL. Again, as we explained in our analysis of categorical decision-making, legibility does not imply human presence at the single deliberation of employing lethal force against a human target. LAWS ensuring a satisfying level of legibility would thus be acceptable under IHRL also absent human intervention in the decision-making process.

3.4. The last issue raised by ATC has to do with another right that is well-accepted today in the field of data protection, namely the individual right not to be subject to a decision *significantly* affecting them based *solely* on an automated processing of their personal data.[52] The need for maintaining human presence in the decision-making process – so far dispensable – would be of some relevance eventually.

The rationale and the scope of this right must be ascertained in the light of the relevant provisions. First, it does *not* qualify as absolute as it is permissible to make exceptions to it in certain cases, notably upon express authorization by the relevant public authorities.[53] However, on closer inspection, relevant provisions are clear in requiring that even in those cases a minimum of safeguard measures must be guaranteed to the affected individuals,[54] among which are: the right to obtain *human intervention*; to express one's point of view; to obtain an explanation of the decision reached after such assessment; and to challenge the decision.[55] Importantly, the notion of "human intervention" can be interpreted in a broad sense, encompassing not only cases in which human intervention is absent in the automated decision-making process, but also cases of *nominal* interventions (i.e. those in which humans exercise no real influence on the outcome of the decision).[56] In other words, human intervention must be *meaningful* for ensuring that the right in question is respected *in concreto*. It must be recalled that such interpretation of human intervention is actually contrasted by some authors, whose take is that also "nominal" human intervention may

52 See GDPR, art. 22(1): «The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her»; Modernized Convention, art. 9(1): «Every individual shall have a right: (a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration»; Explanatory Report, § 75: «It is essential that an individual who may be subject to a purely automated decision has the right to challenge such a decision by putting forward, in a meaningful manner, his or her point of view and arguments».

53 See for instance GDPR, Recital 71 («decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent»).

54 See Explanatory Report, § 75 («However, an individual cannot exercise this right if the automated decision is authorised by a law … which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests»).

55 See GDPR, Recital 71 and 22(1). Importantly, art. 22(1) does not refer to the right to receive explanation, while Recital 71 does; it seems however more appropriate to interpret the former provision in the light of the latter, which is consistent with well-known interpretive criteria.

56 See MALGIERI, COMANDÈ, *Why a Right to Legibility*, cit., p. 251-252 (underscoring how only such interpretation is able to prevent an illegitimate discrimination between «fully automated systems» and «scoring systems» in performing the same activities and potentially producing the same outcome).

be deemed sufficient.[57] Be that as it may, the rationale of the provision is to protect individuals when affected by particular processes, for example "scoring" mechanisms employed by bank when assessing creditworthiness, in order to avoid discriminatory treatment.[58] Such safeguard essentially consists in introducing human components such as *critical sensibility* and *judgment capabilities* in the decision-making process: human discretion is considered as the strongest bastion against discrimination and unfair treatment of data.

Whether such a rationale can be extended (yet *mutatis mutandis*) to ATC is questionable, as the divergence between the former contexts (e.g. credit scoring) and those where LAWS will be operated in our scenario (e.g. law-enforcement operations) may warn against drawing rash and far-fetched analogies. An *a fortiori* reasoning here, albeit appealing, may risk obliterating that divergence. On the one hand, ATC undeniably produces legal effects concerning the individual and «*significantly* affects» him/her, given that it is the very right to life to be at stake.[59] On the other hand, the difference in operational contexts should not be underestimated: law-enforcement agents are often required to take split-second decisions based on the individual's conduct in specific circumstances – in short, where operational tempo may not allow for a human operator to review a decision made by a LAWS.[60] The temporal dimension, in short, can be regarded as a cutting-point element of distinction from other contexts where data processing normally occurs.

The right not to be subject to a solely automated decision is interestingly mirrored in the recently coined notion of Meaningful Human Control (MHC), a veritable *punctum dolens* in the current debate on LAWS.[61] Virtually all States, NGOs and representatives of the civil society consider MHC as the basic requirement for any weapons system, as it requires human deliberation to be present at critical decisions made by LAWS (such as target selection and engagement).

57 See S. WACHTER, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 92 («the phrase "solely" suggests even some nominal human involvement may be sufficient»).

58 See MALGIERI, COMANDÈ, *Why a Right to Legibility*, cit., p. 251.

59 See GDPR, Art. 22(1); for a commentary, see MALGIERI, COMANDÈ, *Why a Right to Legibility*, cit., at 252 (explicitly interpreting the provision as encompassing all practices having any influence on «human rights and constitutional rights of individuals» and pinpointing that such human rights at stake «cannot be considered a "numerus clausus"»).

60 For an appropriate example, see C. HEYNS, *Human Rights and the Use of Autonomous Weapons Systems During Domestic Law Enforcement*, in *Human Rights Quarterly*, 2016, p. 358 (arguing that LAWS programmed with facial recognition software whereby they can use lethal force against an hostage-taker exposing himself for a split second are lawful, as long as the human alternative is suboptimal and human control is ensured over the operation; in these particular circumstances, given the narrow-spatial boundaries of the operation, it does not seem to be at odds with the right to life).

61 For an overview of the notion, its scope and its purposes, see U.N. Institute For Disarmament Research (UNIDIR), *The Weaponization Of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move The Discussion Forward*, 2015, p. 4, http://www.unidir.org/en/publications/the-weaponization-of-increasingly-autonomous-technologies-considering-how-meaningful-human-control-might-move-the-discussion-forward;
CHENGETA, *Defining the emerging notion*, cit., p. 833 ff.. The first conceptualization of MHC has been pushed forward by the British NGO Article 36: see the Report *Key Areas For Debate On Autonomous Weapon Systems*, 2014, available at: http://www.article36.org/wp-content/uploads/2014/05/A36-CCW-May-2014.pdf. The importance of MHC in the debate is captured by C. Heyns, *Autonomous weapons in armed conflict and the right to a dignified life: an African perspective*, in *South African Journal On Human Rights*, 2017, p. 50 (arguing how MHC is perceived as «the dividing line between acceptable and not acceptable machine autonomy»).

However, there regrettably is ample disagreement about how to understand the notion: some consider it necessary to retain a human operator as a general supervisor with little chance to intervene in the single lethal decision (a "broad" understanding of MHC),[62] while others call for a more substantial role played by the human operator (a "narrow" understanding of MHC).[63]

The dichotomy of narrow and broad understandings of MHC reproduces the contrast around "nominal" human intervention in automated decision-making. Notwithstanding the respective different contexts it seems that the underlying rationales of meaningful human intervention relating to the right not to be subject solely to an automated decision and the specific notion of MHC actually overlap. It has been argued that the «major purpose» of a notion of MHC is to fill any possible «accountability gap».[64] Having a human agent in a relationship of control and dependence with LAWS is perceived as the only way to ensure accountability in cases where LAWS's conduct results in a violation of relevant law; a broad understanding of MHC (for example, limited to having a human presence at the act of pre-programming a LAWS) replicates similar drawbacks associated with "nominal" human intervention, namely higher risk of biases,[65] poorer situational understanding, lack of critical sensibility and judgment.[66]

To sum up, it is true that the right not to be subject to solely automated decision-making founds its place in the field of data protection and privacy, and expanding it may seem an improper use of the *a fortiori* argument. However, on closer inspection its rationale is close to the one that inspires the notion of MHC. In both cases, meaningful human presence ensures intervention at the outcome of an automated decision-making process, which allows for the human "component" to be part of the equation. In the case of LAWS, the requirement of MHC reflects the more specific need for accountability in cases where a particular use of force was not permitted.

4. Summarizing what has been argued so far, for ATC to be IHRL-compliant it must: (1) involve data collection only when «strictly necessary» as far as the right to privacy is concerned; (2) employ categories that are consistent with the right to life's requirements of «absolute necessity» and «proportionality»; (3) ensure a sufficient degree of legibility, i.e. an understanding of the actual functioning of the process that leads to the use of force; (4) allow for *meaningful* human intervention to the extent that accountability gaps are eliminated. All these requirements are quite stringent, especially if applied to existing technology; this is why most scholars who contrast the

62 See for instance M. SCHMITT, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, in *Harvard National Security Journal*, 2013, p. 1-38.

63 See for instance N. SHARKEY, *Staying in the loop: human supervisory control of weapons*, in N. BHUTA, S. BECK, R. GEIB, H. LIU, C. KREB (eds.), *Autonomous Weapons Systems*, Cambridge, 2016, p. 34 ff..

64 See CHENGETA, *Defining the emerging notion*, cit., p. 883 and *passim*.

65 For a brief explanation of «automation bias» and risks associated therewith, see CHENGETA, *Defining the emerging notion*, cit., p. 853-854 (concluding that «mere involvement of a human being in the loop» must be rejected as it does not ensure that a human operator retains effective control over the weapon).

66 Paraphrasing MALGIERI, COMANDÈ, *Why a Right to Legibility*, cit., p. 252; see *amplius* CHENGETA, *Defining the emerging notion*, cit., p. 872 ff. (arguing that «the analysis of facts on the battlefield and fitting them to pre-defined parameters» – which is what constitutes «the real decision-making to kill» – is not sufficient for the purposes of MHC, a notion that requires that human agents be «in control of the system for each individual attack because such control is central to establishing the responsibility of combatants»).

development of LAWS are inclined to do so on the basis of their actual feasibility (i.e. technological or pragmatic objection).[67]

There is however an alternative understanding of ATC's implications on human rights, focusing more on the uniqueness of autonomous decision-making as a process where human deliberation may be absent with regard to a *specific* use of force. It is an argument based on *human dignity* – possibly one of the most contrasted, debated notions in the contemporary discourse around human rights.[68] Some scholars argue that the lack of human presence at force delivery against an individual entails a violation of human dignity *as such*, as targets are treated as mere objects.[69] The essence of this kind of arguments lies in that non-human decision-makers «have no understanding of the importance of life, and of the implications of taking it»:[70] emphasis here is therefore not placed on accountability, but rather on the capacity of *understanding* the gravity of a decision. Appealing to concepts such as "human dignity" or "humanity" raises however a bunch of issues, in first place as the meaning of such expressions is contested not only in the legal debate, but also – and foremost – in the moral one.

67 The essence of such objection has been recently captured by HEYNS, *Autonomous weapons in armed conflict and the right to a dignified life*, cit., p. 58: «the requirement of meaningful human control is needed not as a matter of principle, but in order to secure accuracy in targeting and as a basis for legal reform. Clearly, this approach is conditional on technological developments, and may or not be trumped depending on such progress».

68 To recapitulate here the immense literature on this subject would be impossible. Suffice it to recall the following contributions: O. SCHACHTER, *Human Dignity as a Normative Concept*, in *American Journal of International Law*, 1983, p. 848 ff.; J. FROWEIN, *Human Dignity in International Law*, in D. KRETZMER, E. KLEIN (eds.), *The Concept of Human Dignity in Human Right Discourse*, The Hague, 2002, p. 121 ff.; for a ECHR-centered focus, see J. COSTA, *Human Dignity in the Jurisprudence of the European Court of Human Rights*, in C. MCCRUDDEN (ed.), *Understanding Human Dignity*, Oxford, 2014, p. 393 ff..

69 See *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, cit., particularly at § 95 («[d]eploying LARs has been depicted as treating people like "vermin", who are "exterminated." These descriptions conjure up the image of LARs as some kind of mechanized pesticide»); P. ASARO, *Jus Superveniens: robotic weapons and the Martens Clause*, in R. CALO, M. FROOMKIN, I. KERR, *Robot Law*, Cheltenham-Northampton, 2016, p. 385 («this also relates to the question of human dignity. If a combatant is to die with dignity, there must be some sense in which that death is meaningful. In the absence of an intentional and meaningful decision to use violence, the resulting deaths are meaningless and arbitrary, and the dignity of those killed is significantly diminished»); O. ULGEN, *Human Dignity in an Age of Autonomous Weapons: Are We in Danger of Losing an "Elementary Consideration of Humanity"?*, in *ESIL Conference Paper*, 2016, p. 8 («[h]uman targets are denied the status of rational agents with autonomy of will, and arbitrarily deemed irrational agents subject to extrajudicial killings or sub-humans not worthy of human face-to-face contact»). A dignity-based approach is defended by, *inter alios*, the Holy See: see for instance the Statement at the 2017 GGE, unfortunately unavailable on the CCW website: «[a] machine is only a complex set of circuits and this material system cannot in any case become a truly morally responsible agent. In fact, for a machine, a human person is only a datum, a set of numbers among others».

70 See HEYNS, *Autonomous weapons in armed conflict and the right to a dignified life*, cit., p. 58.

To address the issue in a satisfying manner is not possible here; probably the most appropriate conclusion would be at least to leave a door open for a more principled reflection that could take moral considerations into account. This is all the more imperative in a time when humanity faces an unprecedented scenario of «death by algorithm»:[71] the discourse around ATC, the (mis-)use of "big data" and compliance with IHRL can at most *put off* – and not *wipe out* – the intrinsic moral dilemma raised by this new technology and the risks associated thereto.

DIEGO MAURI

71 The quote is from HEYNS, *Autonomous weapons in armed conflict and the right to a dignified life*, cit., p. 48.

I.2

The use of big data as a risk for individual self-determination and the implementation of competition law in the digital market - A comparative approach between the European Union and the United States of America[72]

SUMMARY: 1. Introduction - 2. Human dignity as a fundamental right – 3. The fundamental rights to privacy and to data protection – 4. A short comparison between the European Union and the United States on data protection – 5. Digital and data-driven economy: elements of a same phenomenon – A brief overview on the EU Digital Single Market – 6. Competition law and the control over market power dynamics in digital markets – 7. Conclusions

1. This paper aims at studying two main fundamental rights, namely, the rights to human dignity and to the protection of personal data which, throughout their analysis in the digital context, will be found to be affected by the use of new technologies and the mechanisms of digital economy.

In order to carry out the said analysis the first two paragraphs will investigate the origins and the meaning of the right to human dignity in its sense of self-determination, and to privacy in its narrower notion of personal data protection and will try to demonstrate that both these rights that are currently recognised and protected by the Charter of Fundamental Rights of the European Union (the "Charter" or "CFR") initially took origin from the studies of US scholars and from the interpretive activity of the Supreme Court of the United States ("SCotUS").

The third paragraph will briefly offer some observations on the comparison between the two legal systems of the EU and the US concerning privacy protection.

The fourth paragraph will consider the framework of data driven economy which forms an important part of the digital economy and will particularly play an imperative role in the development of the EU digital single market as craved by the 2020 objectives set out by the European Commission, in order to increase commercial transactions inside and outside the EU economic area.

The final paragraph will explore the possibility to apply competition law (at least, EU competition law – insofar as the EU single market is concerned) with the view to increase competition between firms operating in the digital context and in the meantime to reduce market power of the biggest digital firms. In the concluding paragraph, some remarks on the analogies and differences between the EU and the US legal systems will be made and some solutions to prevent the infringement of the right to self-determination will be suggested.

2. Over the years, human dignity has been differently denoted. Starting from its consideration as an absolute (sometimes even a relative) value[73], it eventually obtained an official

72 This text has been conceived and drafted for the purposes of the participation in the Seminar *Big Data and Public Law: new challenges beyond data protection*, organised by the University of Milan and held in Gargnano (Italy), on 15-17 October 2018. This paper was introduced within Panel 1 – *Big Data and Public Law.*

73 D. SHULZTINER, G. E. CARMI, *Human Dignity in National Constitutions: Functions, Promises and Dangers,* in *The American Journal of Comparative Law*, 2014, p. 470; S. Lieto, *Dignità e "valore" tra etica, economia e diritto,* in *RDPE*, 2013, pp. 163 ff.; M. DÜWELL, *Human dignity: concepts, discussions, philosophical perspectives*, in

recognition as a human right[74]. However, the common ground between its consideration either as a mere value or as a right is represented by its fundamental nature. To be precise, although philosophers and scholars initially estimated it as a non-legal value, dignity was never denied a universal and essential importance, insofar as it was related to the context of human relationships[75]. According to these views, human dignity mainly relates to the individual as observed in his moral relationships with other individuals belonging to the same community he belongs to, and its notion could be easily associated to a concept of «relational dignity»[76].

Starting from this perspective, academics noted that human dignity could manifestly play the role of founding value of any human right[77], even as a sort of a so-called «fundamentally fundamental right»[78]. *Inter alia,* this version has finally been confirmed by the interpretation of human dignity as the unifying trait between the main international documents protecting human

M. DÜWELL, J. BRAARVIG, R. BROWNSWORD, D. MIETH (eds.), *The Cambridge Handbook of Human Dignity*, Cambridge, 2014, p. 29; F. POLITI, *Il rispetto della dignità umana nell'ordinamento europeo,* in S. MANGIAMELI (ed.), *L'ordinamento europeo – i principi dell'Unione*, Milan, 2006, pp. 4 ff.

74 First and foremost through its official recognition in the Preamble of the Charter of the United Nations (1945 – see http://www.un.org/en/charter-united-nations/) and in article 1 of the Universal Declaration of Human Rights (1948 – see http://www.un.org/en/universal-declaration-human-rights/). The philosophical and doctrinal wave which interpreted human dignity as a human right stemmed from the violent events occurred during the II World War, which called for urgent legal measures to the benefit of the individuals. Simone Weil and Hannah Arendt belonged to the said doctrinal wave (see also S. WEIL, *La personne et le sacré*, 1957, cit. in S. Lieto, *Dignità e "valore" tra etica, economia e diritto*, in *RDPE*, 2013, p. 179; S. RODOTÀ, *Il diritto di avere diritti,* Rome, 2012; C. MENKE, *Dignity as the right to have rights: human dignity in Hannah Arendt*, in M. DÜWELL, J. BRAARVIG, R. BROWNSWORD, D. MIETH (eds.), *The Cambridge Handbook of Human Dignity*, cit., p. 332; S. BAER, *Dignity, liberty, equality: a fundamental rights triangle of constitutionalism*, in *University of Toronto Law Journal*, 2009, p. 443; C. DUPRÉ, *The Age of Dignity*, London, 2015, pp. 37 ff.).

75 Worth to be mentioned are some of the theories on human dignity supported by Aristotle, according to whom any individual is endowed with dignity, although all individuals may not be equally respectable depending on the fact that they make actions to the benefit of other people (U. VINCENTI, *Diritti e dignità umana*, Bari-Rome, 2009, pp. 7 ff. in C. SCOGNAMIGLIO, *Dignità dell'uomo e tutela della personalità*, in *Giustizia Civile*, 2014, pp. 67 ff.). This perspective had partially been adopted by the Romans, who considered human dignity as a natural gift (P. BECCHI, *Il principio dignità umana*, Brescia, 2009, in C. SCOGNAMIGLIO, *Dignità dell'uomo e tutela della personalità*, cit., pp. 67 ff.) and later by Kant who based his concept of dignity upon his analysis of the «*moral law*» allowing the human being to be considered never simply as a means but always at the same time as an end [I. KANT, *The Metaphysics of Morals (II. Metaphysical first principles of the doctrine of virtue*), Cambridge, 1996].

76 F. SCARAMELLA, *La dimensione relazionale come fondamento della dignità umana*, in *Rivista di filosofia del diritto*, 2013, pp. 305-320; B. MALVESTITI, *La dignità umana dopo la "Carta di Nizza". Un'analisi concettuale*, Naples-Salerno, 2015; K. T. GALVIN, L. TODRES, *Dignity as honour-wound: an experiential and relational view*, in *Journal of Evaluation in Clinical Practice*, 2015, pp. 410-418.

77 E. DUBUOT, *La dignité dans la jurisprudence de la Cour de justice des Communauteés européennes*, in L. BURGUOGUE-LARSEN (ed.), *La dignité saisie par les juges en Europe,* Brussels, 2010, p. 82; S. PEERS, T. HERVEY, J. KENNER, A. WARD (eds.), *The EU Charter of fundamental rights: A commentary,* London, 2014, pp. 21-23.

78 This expression is used by Burkhert for the right to privacy, but could be used by analogy for defining the right to human dignity in the sense intended by Dupré and Ruggeri. See H. BURKHERT, *Dualities of privacy – An Introduction to 'Personal Data Protection and Fundamental Rights'*, in M. V. PEREZ ASINARI, P. PALAZZI (eds.), *Challenges of Privacy and Data Protection Law*, Brussels, 2008; C. DUPRÉ, *The Age of Dignity,* cit.*;* A. RUGGERI, *Alla ricerca del fondamento dell'interpretazione conforme*, in *Forum di Quaderni costituzionali Rassegna,* available at http://www.forumcostituzionale.it/wordpress/images/stories/pdf/documenti_forum/paper/0056_ruggeri.pdf.

rights, until the value at stake has been included, in 2009, as a formal and first fundamental right recognised and protected by the CFR[79], so underlining its leading importance.

For the first time in the history of existing legal systems human dignity has explicitly been proclaimed as a right and was given an absolute inviolable nature: in other words, in principle, this right could not be limited by the exercise or the protection of other – even fundamental – rights[80]. Nevertheless, at least in the European Union, the express provisions of article 1 of the Charter did not allow its interpreters to concretely and easily safeguard the concerned right by directly applying its precept, by reason of the circumstance that the norm is quite general and indefinite. As a matter of fact, by stating that *«[h]uman dignity is inviolable. It must be respected and protected»*, the Charter only foresees a passive behaviour to respect the individuals' exercise of the right to human dignity and an active conduct in taking any action to protect individuals from potential threats in the exploitation of the above right[81].

However, by doing so, human dignity is not defined and remains a vague notion[82]. As occurred for its inclusion in the Universal Declaration of Human Rights, in the CFR human dignity has not been defined. For this reason, scholars use to affirm that legislators did not specified it intentionally so as to confer dignity with a general concept that could be fit for any necessary practical meaning[83]. Indeed, in line with this theory, the notion of dignity could be articulated into different meanings and forms with the view to protect different practical situations, but above all to include all the other fundamental rights within the wide boundaries of the right that protects them. This would then be possible in the light of its *omnibus* connotation as founding right of the other fundamental rights.

However, on the other side of the Atlantic Ocean human dignity is not expressly embedded in the Constitution. Nonetheless, the United States have a longstanding tradition in protecting dignity through the interpretative activity of the SCotUS which is familiar with including such a value under the framework of the so-called "mother rights"[84]. Such essential rights may not result in being expressly protected by the US Constitution, but they obtain judicial safeguard thanks to the construction granted by the supreme judges who are vested with the power to create binding precedents according to the *stare decisis* doctrine. Some of the manifest cases where the SCotUS recognised a right as being a mother-right (notwithstanding the fact that it was not expressed in the

79 Article 1 of the Charter of Fundamental Rights of the European Union, OJ 2012, C 236 (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN).

80 In this sense, see the judgment of the ECJ of 14 October 2004, *Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbeurgermeisterin der Bundesstadt Bonn*, C-36/02, ECLI:EU:C:2004:614 (see http://curia.europa.eu/juris/showPdf.jsf?text=&docid=49221&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=660433). However, in weighting conflicting fundamental rights, article 52 of the Charter, which provides for the so-called "safeguard clause", always needs to be taken into account. For an in-depth analysis, see S. RODOTÀ, *Il diritto di avere diritti,* Rome, 2012, pp. 31 ff.

81 In this sense and concerning the right to privacy, see H. BURKHERT, *Dualities of privacy – An Introduction to 'Personal Data Protection and Fundamental Rights',* cit.

82 See also F. POLITI, *Il rispetto della dignità umana nell'ordinamento europeo,* cit., p. 58.

83 D. SCHULZTINER, G. E. CARMI, *Human Dignity in National Constitutions: Functions, Promises and Dangers,* in *The American Journal of Comparative Law*, 2014.

84 See also, S. BAER, *Dignity, liberty, equality: a fundamental rights triangle of constitutionalism,* cit.

Constitution) specifically concerned the right to privacy, which thus got an acknowledgment at a constitutional level[85]. In the light of these precedents and according to the doctrine which reconnects dignity to the general category of the right to liberty – under which also the right to privacy falls[86] –, even human dignity as acknowledged by the US judges may be construed as a founding value. In *Lawrence v. Texas*[87], which is a peculiar case of the US jurisprudence, the SCotUS went through the notion of dignity even more markedly, justified it in relation to the concept of privacy and held that dignity may also be articulated into its meaning of one's freedom to decide autonomously and, thus, in one's freedom of choice and self-determination[88].

This is the reason why some scholars tend to state that the American notion of dignity resembles to a value, whereas its EU concept is now undisputedly recognised as a fundamental right and should benefit from a greater protection[89]. The same goes for the protection of the right to privacy and to data protection which is not part of US Constitution (and is therefore safeguarded by judicial interpretation), whilst in the EU it is formally acknowledged and implemented as a fundamental and inviolable right.

Regardless of the above-mentioned theory, it is however important to admit that the US have a strong tradition of human rights judicial protection and that some of the most important rights which have then been included in the respective legislative acts, even in the EU, took origin from US conceptions of the same rights. This is all the more true when the right to privacy is concerned, as it will be shortly analysed below.

3. As anticipated in the first paragraph, the right to privacy is a patent example of how American case-law and scholars have had an impact on the recognition and the implementation of fundamental rights which then influenced their notion in the EU. As a matter of fact, the concept connected to the general right to privacy was created in early 1890 by the two eminent American scholars Warren and Brandeis who basically defined privacy as *«the right to be let alone»*[90]. This doctrine takes its cues from the distinction between privacy – *i.e.* the legal asset needing to be

85 *Ex multis,* see cases *Roe v. Wade*, 410 USA, 113 (1973), *Griswold v. Connecticut*, 381, USA 479 (1965).

86 A. BARAK, *Human Dignity: The Constitutional Value and the Constitutional Right,* in C. MCCRUDDEN (ed.), *Understanding Human Dignity,* Oxford, 2013, p. 186.

87 539 US 558 (2003).

88 N. RAO, *On the use and abuse of dignity in constitutional law,* in *Columbia Journal of European Law,* 2008, p. 240.

89 G. BOGNETTI, *The concept of human dignity in European and US constitutionalism*, in G. NOLTE (ed.), *European and US Constitutionalism*, Cambridge, 2005; ; D. SHULZTINER, G. E. CARMI, *Human Dignity in National Constitutions: Functions, Promises and Dangers,* cit., pp. 470 ff.

90 This definition originated from a case involving Mr. Warren's wife and the publication of some of her pictures made by means of a newly-created Kodak camera. Mr. Warren's wife did not want to be affected from a reputational, social and personal damage, which would have been originated by the circulation of pictures allowed by the use of new technologies. For an in-depth analysis, see A. RENGEL, *Privacy in the 21st century*, Studies in Intercultural Human rights, Leiden-Boston, 2013; K. LACHANA, *Elements of convergence in the historical origins and ideological foundations of the US and European privacy law: the nexus between the "right to be let alone" and continental jurisdictions,* in M. BOTTIS (ed.), *Privacy and Surveillance, Current aspects and future perspectives,* Athene, 2013, pp. 24-44; L. MIGLIETTI, *Il diritto alla privacy nell'esperienza giuridica statunitense*, Naples, 2014, pp. 19 ff.; M. K. OHLHAUSEN, A. P. OKULIAR, *Competition, Consumer Protection, and The Right [Approach] to Privacy,* in *Antitrust Law Journal,* 2015, pp. 125 ff.

protected by the legal system – and the right to privacy – *i.e.* the legal tool by which the legal asset can be safeguarded[91].

In truthfulness, Warren and Brandeis were not the first ones to theorise the right to privacy, because in 1834 Justice Cooley, judge of the SCotUS, ruled over a case on tort law and – quite by chance – examined the matter of an individual's privacy by deeming that the *«right to one's person may be said to be a right of complete immunity: the right to be let alone»*[92]. However, it was only with Warren and Brandeis that privacy and its connected rights were considered in the perspective of the need for the individual to take some aspects of his life secret and confidential, with no intrusions from other people. Therefore, only 1890 could be universally considered as a "cut-off" date for the formal acknowledgement and recognition of the right to privacy[93].

Only afterwards, this brand new legal concept started to be exported to Europe and then to the European Union[94]. Scholars also began to analyse the level of a «*reasonable expectation of privacy*» which is useful for legislators and judges to identify a general and adequate definition of the right to privacy that could be valid for any individual, thus not associated with a subjective and personal perception of the need to be let alone[95]. Thanks to this doctrine, the European Convention on Human Rights included the right to privacy, as worthy to be safeguarded as a human right[96].

Nowadays, despite the quite negative meaning which some philosophers tried to give to privacy[97], it is nowadays widely accepted by scholars that the concept of privacy (and accordingly that of the relevant right to privacy), just like the one of dignity, is a sort of an «umbrella concept» embedding many definitions which generally refer to positive connotations identifying multiple details of an individual, that the latter wishes to preserve as confidential and not to disclose to others[98]. As a result, even the notion of the right to privacy may embrace different denotations and may be applied differently depending on the context it refers to.

91 A. RENGEL, *Privacy in the 21st Century*, cit., p. 31.

92 T. C. COOLEY, *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, Chicago, 1879; R. B. STANDLER, *Privacy Law in the U.S.A.,* 1997, retrieved from http://www.rbs2.com/privacy.htm; N. LUGARESI, *Internet, Privacy e Pubblici Poteri negli Stati Uniti,* Milan, 2000, p. 49.

93 M. K. OHLHAUSEN, A. P. OKULIAR, *Competition, Consumer Protection, and The Right [Approach] to Privacy,* cit., p. 126.

94 See the commentary on article 8 of the CFR by Bassini and Pollicino. M. BASSINI, O. POLLICINO, IN S. ALLEGREZZA, R. MASTROIANNI, F. PAPPALARDO, O. POLLICINO, O. RAZZOLINI (eds.), *Carta dei diritti fondamentali dell'Unione europea*, Milan, 2017, p. 135.

95 J. L. MILLS, *Privacy the lost right*, Oxford, 2008, pp. 20 ff.; D. J. SOLOVE, *Understanding Privacy*, Cambridge, MA, 2008, pp. 71 ff. This tendency started from the well-known case *Katz v. United States* (389, US 347, 360, 1967) where Justice Harlan stated *«[a] person has a constitutionally protected reasonable expectation of privacy...[T]here is a two-fold requirement, first that a person have exhibited an actual [subjective] expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable" [...]».*

96 European Convention on Human Rights, signed in Rome on 4 November 1950 (see https://www.echr.coe.int/Documents/Convention_ENG.pdf).

97 For instance, the above cited Hannah Arendt held that the fact that the individual has privacy means that he is deprived of something. Therefore some definitions of privacy were provided with a negative connotation, instead of the positive attitude that the right to privacy attempts to underline. See D. J. SOLOVE, *Understanding Privacy*, cit., pp. 80 ff.

98 D. J. SOLOVE, *Understanding Privacy*, cit., p. 45; see also D. J. SOLOVE, *Nothing to Hide – the False Tradeoff between Privacy and Security*, New Haven, 2011, pp. 24 ff.; e J. E. COHEN, *What privacy is for,* in *Harvard Law Review,* 2013, p. 1908.

Worth to be particularly mentioned are two of the multiple definitions offered by academics. Namely, two American researchers, Westin and Solove, have studied the right to privacy more recently and confirmed that – indeed – it deals with a multifaceted and complex human perspective, so that it must be conceived at a general level in order to include all the possible concrete situations. However, both Westin and Solove believed that one of the most interesting and important aspects of the right to privacy deals with the protection of oneself's information, that is to say with the faculty to decide whether and how to disclose personal data to third parties and to which purposes[99]. The said doctrinal tendency, which has been developing almost simultaneously with the rise of new technologies (that let data flow easier and much quicker than before), led European judges to detect a separate fundamental right formally recognised for the first time by the Nice Charter[100], then replaced by the binding CFR in 2009[101]. Hence, to date the European Union seems the first legal system where the right to data protection is safeguarded as a fundamental right[102], moreover in a distinct manner as compared to the broader right to privacy.

Still, in spite of its narrower definition, even the right to data protection agrees to be articulated into various forms. One of the most interesting classification conceived by scholars involves the models of informational privacy, on the one hand, and of decisional privacy, on the other. The said division is reckoned to be derived from a passive and an active understanding of privacy. As a matter of fact, informational privacy would be approached to a rather passive behaviour of the data subject (the individual whose data may be disclosed[103]) and this would also be

99 D. J. SOLOVE, *Introduction: Privacy Self-Management and the consent dilemma*, in *Harvard Law Review,* 2013, p. 1882; D. J. SOLOVE, *Understanding Privacy,* cit.*;* A. WESTIN, *Privacy and Freedom*, in *Washington and Lee Law Review*, 1968.

100 Formally, the Nice Charter (see https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):IT:HTML) had exactly the same content as the Charter of fundamental rights, but acted as a soft law instrument until its entry into force and the entry into force of the Lisbon Treaty on 1st December 2009 (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=EN).

101 Certainly, the right to data protection had expressly been included in Convention no. 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – see https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37) signed within the framework of the Council of Europe in 1981, entered into force in 1985 and currently ratified by 43 States. This Convention is said to have built a sort of «golden standard» as it sets out different rights connected to the right to data protection which are implemented also in the more recent legal acts for the safeguard of the individuals in exercising their right to the protection of personal information (see F. W. HONDIUS, *A quarter century of international data protection,* in *Hague Yearbook of International Law,* The Hague, 2005, p. 31).

102 Article 8 reads as follows *«1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by and independent authority».*

103 «Data subject» is a definition taken from the newly entered into force EU GDPR, *i.e.* 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), OJ 2016, L 119, pp. 1-88 (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1543829083725&from=EN), in particular from its article 4, number 1, which reads as follows: *«"personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors*

confirmed by US scholars after a series of judgments which needed to construe the fifth and the fourteenth amendments of the US Constitution and that ruled that it was convenient to differentiate the personal interest in preventing the disclosure of one's personal data from that to make decisions in a total autonomous manner[104]. This last connotation would call for a more active conduct – *i.e.* to independently take decisions – which is rather connected to the decisional nature of privacy. Then, whereas the informational privacy is clearly protected, for instance in the EU by the CFR, the decisional aspect of privacy cannot be asserted as an express fundamental right. It could however be recognised as an inviolable right by considering the right to data protection (and thus to privacy) together with the right to human dignity, and supposing that these two crucial rights are suitable to be melted into a single freedom which is the right to self-determination, while protecting one's own intimacy and identity. The freedom to self-determinate means the faculty to decide whether and how to disclose personal data, which kind of data to unveil and for which purposes[105].

In the end, the above theory caused legal interpreters to create a contemporary and innovative right represented by the so-called right to *informationnelle Selbstbestimmung* (or informational self-determination)[106]. This concept has been employed by the German *Bundesverfassungsgericht* in a judgment issued in 1983, where it was acknowledged as *«the power of the individual to decide in a substantial autonomous manner about the assignment and use of his personal data»*[107] thanks to the exploitation and interpretation of article 1 of the German Constitution which protects human dignity as an inviolable value. Henceforward, the original definition of informational self-determination is able to definitely confirm the direct connection between the right to human dignity and the right to privacy and data protection. Moreover, given that the above-mentioned concept has been developed due to the works of academics and jurisprudence across the American and the European continents, it should be useful to compare the two legal systems on the safeguard of the right to data protection, because some differences should be stressed in order to proceed in the analysis of data-driven economy carried out in the fifth paragraph.

4. In terms of protection of the rights to privacy and to data protection, the European Union and the United States tend to apply different principles in the light of, especially, the aspects outlined below.

Firstly, significant divergences are seen in their express recognition as fundamental rights. Indeed, in addition to have granted the two rights at hand a constitutional warranty, thanks to their

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person».

104 See judgment in *Whalen c. Roe*, 429 U.S. 589, 598-600 (1977) where the SCotUS expressly referred to *«the individual interest in avoiding disclosure of personal matters, and [...] the interest in independence in making certain kinds of important decisions».* See H. BURKHERT, *Introduction. Dualities of Privacy – An Introduction to "Personal data Protection and Fundamental Rights"*, cit., pp. 20 ff.; N. J. King, *Fundamental Human Right Principle Inspires U.S. Data Law, but protections are less fundamental,* in M. V. PÉREZ ASINARI, P. PALAZZI (eds.), *Cahiers du CRID,* n. 31, *Défis du Droit à la Protection de la Vie Privée – Challenges of Privacy and Data Protection Law*, Brussels, 2008, pp. 79 ff.

105 N. J. KING, *ibidem.*

106 G. SARTOR, *Tutela della personalità e normativa per la "protezione dei dati"*, in *Informatica e diritto*, 1986, XII.

107 Courtesy translation. See G. SARTOR, *ibidem*.

inclusion in the CFR[108], the EU has recently adopted a unique legal framework (the General Data Protection Regulation – GDPR[109]) for the protection of personal data of any natural person, regardless of the fact that such a person is a EU citizen or not[110]. Being a regulation, the GDPR is directly applicable in the same manner in every Member State and thus guarantees the full harmonisation of its provisions within the EU[111], but data protection also benefits from other EU legislative acts adopted for being implemented in different contexts (*e.g.* criminal investigations[112]). Secondly, on the American side, the US Constitution does not formally provide for any right to privacy or to data protection, but these ones are basically protected through the interpretative work of the SCotUS, which has often been called to construe the fourth, the fifth and the fourteenth amendments with the purpose to protect individuals from harms to their privacy[113]. Thirdly, differently from the EU, the United States do not grant a uniform safeguard of individuals' privacy, because they cannot profit from a harmonised legal framework (this legislative sector is indeed characterised by a strong fragmentary nature, due to the fact that every legislative act concerns a different social, political or economic sector[114]). Fourthly, the main interesting discrepancy concerns

108 Article 6 of the Treaty on the European Union (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016M/TXT&from=EN), as amended by the Lisbon Treaty, now provides the Charter with the same legal value as the founding Treaties.

109 See footnote 103 above.

110 Indeed, the GDPR applies regardless of the data subjects' origins when data is processed either in the EU or outside the EU when (i) the controller or the processor are anyway based in the EU, (ii) the processing made outside the EU handles data from EU citizens (article 3 of the GDPR). This is also known as the extraterritoriality principle of EU data protection. See, *ex multis,* J. P. ALBRECHT, *Uniform Protection by the EU – The EU Data Protection Regulation Salvages Informational Self-determination*, in H. HIJAMNS, H. KRANENBORG (eds.), *Data Protection Anno 2014: How to Restore Trust?*, Mortsel, 2014, pp. 122 ff.; F. FABBRINI, *Privacy and National Security in the Digital Age*, in *Tilburg Law Review, Journal of International and European Law*, 2015, p. 8; C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Bologna, 2015, p. 146.

111 R. ADAM, A. TIZZANO, *Lineamenti di diritto dell'Unione europea*, Turin, 2010.

112 See Directive 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, OJ 2016, L 119, pp. 89-131 (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&qid=1543829334357&from=EN). Another important act which is now under the scrutiny of the Council of the EU for its adoption is the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications – see https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN) which will be meant to replace Directive 2002/58/EC on electronic communications that now seems quite obsolete for a complete protection of consumers' and individuals' personal data in their electronic communications and transactions (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&qid=1543829428945&from=EN). This regulation is also known as the «*e-privacy regulation*».

113 K. LACHANA, *Elements of convergence in the historical origins and ideological foundations of the US and European privacy law: the nexus between the "right to be let alone" and continental jurisdictions*, p. 29; L. MIGLIETTI, *Il diritto alla privacy nell'esperienza giuridica statunitense,* cit., p. 27; A. RENGEL, *Privacy in the 21st Century,* cit.

114 Some of the most known US legislative acts on privacy issues are the *Freedom of Information Act - FOIA* (1966), the *Privacy Act* (1974 – see https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf), the *Computer Matching and Privacy Protection Act* (1988), the *E-FOIA* (1996 – see

an academic achievement which relates to the circumstance that the US tend to exclusively protect the privacy of their own residents. Conversely, the EU provides for privacy safeguard for any individual, given that it includes the relevant right in the Charter and, therefore, grants to any natural person and not exclusively to its citizens[115]. Simultaneously, scholars began to think that, for the above said reason, the rights to privacy and to data protection in the EU would be directly connected to the protection of human dignity, recognised in favour of any human being. On the other hand, commentators believed that the US cover privacy needs in a manner that is instead associated to the implementation of liberties[116].

This peculiar achievement reached by legal researchers represents an important milestone in this brief analysis, because dignity will henceforth be considered as aimed at protecting any and all individuals, even regardless of their economic and market role. To the contrary, by referring to liberty, a considerable role would be deemed to be played by market structure where only consumers – who are natural persons[117] – seem to be protected.

According to scholars, the foregoing would probably mean that the EU legal system would better protect individuals than the US one, because in principle, the EU worries more about individuals, whereas the US tend to mainly care about markets, profits and, thus, consumers, mostly disregarding individuals that are neither consumers, nor American citizens[118]. However, from a political perspective, this would not be completely correct, because the previous observations emerge from a European point of view, in the light of which Europe has traditionally been built not only upon economic liberties, but also on the compliance with human rights. Conversely, such a theory starts from social and political needs different from those which led to the development of the US legal system that, in any case, must be recognised as safeguarding human rights, although their definitions could vary if compared to their respective denotations in the EU. Nonetheless, such a divergence would not necessarily mean that a legal system is superior to the other one[119]. Suffice it to say that also freedom to conduct a business is recognised by the CFR and may sometimes require a balancing with other fundamental rights, since it may contrast with individuals' and, in particular, consumers' rights[120].

Without going further into detail in the analysis of the comparison between the EU and the US on this issue, Susan Baer's theory on the constitutional triangle should be evoked, as it could give precious hints for the development of this research. As a matter of fact, the above legal model makes an attempt in maintaining that, in most legal systems, a constitutional triangle of values may

https://www.justice.gov/oip/freedom-information-act-5-usc-552 and also https://www.foia.gov) and the *Patriot Act* (2001 – see https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf). For an in-depth analysis see *inter alia*, L. MIGLIETTI, *Il diritto alla privacy nell'esperienza giuridica statunitense,* cit.; U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milan, 2008; A. RENGEL, *Privacy in the 21st Century,* cit.

115 M. MILANOVIC, *Human rights treaties and foreign surveillance: Privacy in the digital Age*, in *Harvard International Law Journal*, 2016, *inter alia,* pp. 100 ff.

116 J. Q. WHITMAN, *"Human dignity" in Europe and the United States: the social foundations*, in G. NOLTE (ed.), *European and US Constitutionalism*, Cambridge, 2005.

117 However, it is necessary to specify that not every individual could be a consumer.

118 G. BOGNETTI, *The concept of human dignity in European and US constitutionalism*, cit.

119 See J. Q. WHITMAN, *"Human dignity" in Europe and the United States: the social foundations,* cit., p. 124.

120 For the sake of clarity, for in the EU, consumers are granted with the inviolable right to profit from a high level of protection – article 38 of the Charter.

be identified. The values upon which the said triangle is built are dignity, liberty and equality, even if they can be conflicting. In any case, none of these three values could be disregarded by the concerned triangle, because there are three angles and each one of them is ideally filled with one of the above clarified values. What is subject to change is the flexibility of the inclination of the angles that, if legally translated, may vary according to the bigger importance recognised to dignity or to liberty or, still, to equality[121]. Eventually, the foregoing would mean that dignity could be underestimated in favour of liberty or of equality or *vice versa*, but in no event one of the values could be expunged to benefit the other two. Then, according to the above view, the EU and the USA legal systems could be based upon different constitutional triangles and give more relevance either to dignity or to liberty. But the two of them[122] are forced to implement such a triangle in any social, political or economic context.

Baer's theory allows us to introduce the final part of this research concerning the issue of data-driven economy, insofar as the above specified principles bearing the constitutional triangle theory should equally be applied in the digital context, despite the fact that digital economy has potentially no territorial and legal boundaries. It will be understood how the principle of extraterritoriality enshrined by the EU GDPR will come to the aid of the reader.

5. The 2020 Europe Strategy envisaged by the European Commission in early 2010 includes the Digital Agenda[123] among its seven main pillars. By the end of 2020, the said Agenda should largely be implemented thanks to the expansion and the increase of the Digital Single Market, basically retracing the building principles of the European Single Market because of which, *inter alia*, original Member States agreed the constitution of the European Communities.

Not only the EU economy, but also global economy is nowadays facing the challenges brought by the web. In particular, keeping on developing through it, digital economy could be said to be mostly functioning by means of the ceaseless flow of data. Such data is mainly represented by personal information belonging to web users. In this respect, it is no secret that in the last years the European digital market has lived a boost largely thanks to the flow and the processing of web users' and non-users' personal data and this is also the reason why the EU legislator believed to take even deeper steps in the regulation of individuals' data flows and processing with the new GDPR: not surprisingly, even the title of the GDPR demonstrates that it is specifically addressed to simplify the free movement of personal data[124].

It is strongly believed among academics that personal data is the raw material upon which most part of global economy currently works, but it also is a sort of currency that can be given in exchange for other services or goods that are apparently free[125]. Nonetheless, although data has

121 S. BAER, *Dignity, liberty, equality: a fundamental rights triangle of constitutionalism,* cit.

122 Actually, three of them if considered with equality.

123 See Digital Agenda website (see https://ec.europa.eu/digital-single- market/en/europe-2020-strategy) and the objectives of the Digital Single Market (see https://ec.europa.eu/commission/priorities/digital-single-market_en).

124 See also, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Building a European data economy*, 10 January 2017, COM(2017) 9 final, p. 5 (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN).

125 *Inter alia,* see F. PANAGOPOULOU-KOUTNATZI, *Facebook as a challenge to privacy*, in M. BOTTIS (ed.), *Privacy and Surveillance, Current aspects and future perspectives*, Athene, 2013, p. 217; A. ACQUISTI,

gained a monetary value, it always has a personal intimate value of the person to whom it belongs to[126]. Such a personal significance is however subject to the risks of unsolicited and undesired intrusions by third parties of which concerned data subjects are either unaware or not well informed. Indeed, through the collection of single personal data, or of even small sets of personal information, and by means of the automated mining and combination of such information, huge amounts of personal details may be directly or indirectly made available to third parties, that can ultimately use them for economic purposes. These massive groups of data are currently named as "Big Data" and are created by the combination of single pieces of information, collected and generally used to derive predictive information on single individuals and social groups[127]. They are well-known for being easy to collect and combine and for being characterised by the so-called 3Vs (Volume, Velocity and Variety)[128].

Therefore, Big Data constitutes the biggest innovation of this decade, because it can serve the "customisation" function useful to adapt any service or product to the specific needs of any single individual, whose data is collected, processed, analysed and combined[129]. This option is mostly used in real or virtual market dynamics, and holders of such data do have a decisive impact on consumers' choice if they use them or make someone other use them to drive sales and consumptions. It is not forcedly a negative impact, because consumers could get more benefits from buying something that is more coherent with their personal needs. However, consumers may also be concerned by the fact that their information is collected, then combined and maybe assigned to third parties, regardless of an express and completely conscious consent in that regard[130], to the detriment of their self-determination.

Moreover, data-driven economy also raises some issues concerning the possible commercial deals that see personal data as their main object. It is hereby referred to possible data transactions between interested parties, which basically confirm the nature of personal data as economic assets that can be subject to assignments for free or as a result of a sale. Since these are significant concerns especially felt by data subjects (whether they are individuals or consumers), public institutions should address users' worries in a fair manner taking into consideration both the data subjects' need to be protected in their intimacy and the demands of the market for more information

J. GROSSKLAGS, *What Can Behavioral Economics Teach Us About Privacy?,* in *Digital Privacy: Theory, Technologies and Practices,* 2007, retrieved from https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf; M. J. BECKER, *The consumer data revolution: The reshaping of industry competition and a new perspective on privacy,* in *Journal of Direct, Data and Digital Marketing Practice,* 2014; N. M. RICHARDS, *The dangers of surveillance,* in *Harvard Law Review,* 2013, p. 1938; C. J. HOOFNAGLE a.o., *Behavioural Advertising: the offer you cannot refuse,* in *Harvard Law and Political Review*, 2012, pp. 273-279.

126 F. COSTA CABRAL, O. LYNSKEY, *Family Ties: The Intersection between Data Protection and Competition in EU Law,* in *CMLR,* 2017, pp. 12 ff.

127 See, *ex multis*, C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, cit., p. 45; A. MANTELERO, *Competitive value of data protection: the impact of data protection regulation on online behaviour*, in *International Data Privacy Law,* 2013, p. 231.

128 N. P. SCHEPP, A. WAMBACH, *On Big Data and Its Relevance for Market Power Assessment,* in *Journal of European Competition Law & Practice,* 2016. Some scholars held that another "V" should be added and would stand for their «added Value» compared to a single piece of information (see, Focarelli, *La privacy. Proteggere i dati personali oggi*, cit.).

129 *Ibidem.*

130 *Ibidem.*

in the light of its free movement, provided that data is legitimately collected[131]. Accordingly, the foregoing justifies the duty for public authorities to keep on monitoring market players so that, first, they comply with data protection rules and, second, they act in the framework of completely fair market conditions.

6. One of the goals of this paper is to demonstrate that competition law could play a bigger role in the protection of web users' and consumers' personal data. Indeed, according to what has been pointed out in the previous paragraph, it may seem evident that market players and fair functioning of market dynamics are of an utmost importance even for digital economy based on the continuous flow of personal data. This is all the more clear for the two observations described below.

Firstly, one of the main targets of competition law is consumers' protection (that, as already underlined, has also been upgraded to a fundamental right by the CFR)[132] and pursuant to the definition given by EU law to a consumer, this is *«any natural person who [...] is acting for purposes which are outside his trade, business or profession»*[133]. This essentially means that any consumer is, at the same time, an individual benefitting from inviolable rights, who could also be a web user and a consumer in his digital economic transactions, although such transactions are characterised by the mere exchange of personal data for services which are only apparently free of charge. At any rate, the said exchange has a considerable economic significance that is often imperceptible to the user[134] and this is also the reason why data holds quite an immeasurable competitive value to the market for the market players using it[135].

Secondly, another goal of competition law is to monitor market dynamics in order to create fair and competitive conditions for any undertaking, which means that at the end of any economic process, consumers can profit from better economic conditions. The abovementioned targets of competition law are equally applicable to the digital market where real firms operate in an electronic context to make profits and increase their turnovers.

As mentioned before, digital market is more and more characterised by the huge phenomenon of data collection. Suffice to remind the case of two-sided or multi-sided markets[136] or of search engines, which let suppliers and consumers keep in touch more easily and make the

131 As stated by the European Commission in its Communication of 2014, *Towards a thriving data-driven economy*, SWD(2014) 214 final (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0442&from=FR).

132 F. COSTA CABRAL, *The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law,* in *Maastricht Journal,* 2016, pp. 495-513; A. BARENGHI, *Diritto dei consumatori,* Milan, 2017, pp. 3 ff.

133 Article 2, paragraph 1, letter b), directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993, L 95, pp. 29-34 (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0013&qid=1543829645563&from=EN).

134 According to a recent survey, personal data is given a very insignificant economic value by its "owners", in spite of the greater monetary value it has for third parties collecting and combining it. That research has been carried out by the Financial Times and its results have been later published on Sole24Ore on 14 June 2013, in the article *Big data: tre profili a confronto sul valore dei dati personali* (see http://www.ilsole24ore.com/art/tecnologie/2013-06-14/data-profili-confronto-012622.shtml?uuid=AbTdmq4H).

135 A. MANTELERO, *Competitive value of data protection: the impact of data protection regulation on online behaviour*, in *International Data Privacy Law,* 2013, pp. 229-238.

supply and demand process quicker, at the same time collecting great amounts of personal data both from suppliers and from consumers. Digital platforms – like search engines or digital markets – are usually owned and managed by big digital companies and, in view of the number of users they attract and of their reputation, such companies may have questionable positions on the EU market (that is hereby mainly object of analysis) in the light of competition law. In the recent past, this branch of law – which in the US is more known as antitrust law[137] – has however served to detect potential infringements on the digital market by big digital companies such as, *inter alia,* Google, Facebook, Microsoft or Yahoo!. In fact, it is no coincidence that these giant multinational companies gained important market shares all over the world thanks to the permanent growth of their users.

But alongside with the increase of the number of users, there has also been a bigger availability of personal data that allowed these companies holding a greater competitive value than less notorious or smaller companies.

As a consequence, in the last years, antitrust authorities have shed a light on potential antitrust conducts and, not surprisingly, investigations involved the same undertakings even in the different legal systems of the EU and of the USA[138]. Most of these investigations concerned merger cases[139], where the European Commission and the US Federal Trade Commission were asked to

136 G. LUCCHETTA, *Is the Google Platform a two-sided market?*, retrieved from http://ssrn.com/abstract=2048683. Moreover, it is important to stress that this kind of digital platforms increase their incomes and activities day-by-day only thanks to the so-called positive «*feedback loop*» created by their users, when they use the service of the platforms and they give a public positive feedback about the supply they received. On "feedback loops", see also N.P. SCHEPP, A. WAMBACH, *On Big Data and Its Relevance for Market Power Assessment,* in *Journal of European Competition Law & Practice,* 2016, pp. 121 ff.

137 It is however to be reminded that scholars strongly recognise the origins of EU competition law in US antitrust law, which supplied the basic models to identify illegitimate conducts on the market by undertakings, such as non-allowed cartels or abuses of dominant position on the market, as well as problematic mergers between companies. See J. KLEIN, P. M. RAO, *Competition and consumer protection in the cyberspace marketplace,* in *20th ITS Biennal conference: The Net and the Internet – Emerging Markets and Policies*, Rio de Janeiro, 2014, pp. 4 ff.

138 It is hereby convenient to only mention some of the cases opened by the EU and the US antitrust authorities (respectively, the European Commission and the Federal Trade Commission). For the EU, see case COMP/M.5727 *Microsoft / Yahoo! Search Business* (see *https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543829834283&uri=CELEX:32010M5727*), case COMP/M.7217, *Facebook /Whatsapp* (see https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543829865420&uri=CELEX:32014M7217), case COMP/M.6281, *Microsoft/Skype* (see https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543829888874&uri=CELEX:32011M6281), case COMP/M.4731, *Google/DoubleClick* (only available in summary – see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008XC0722(03)&from=EN). For the US, see FTC file no. 071/0170, case *GoogleDoubleClick* (see https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf), for the merger Facebook/WhatsApp, see FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition, 10 April 2014 (see https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed), and EPIC press release of 25 August 2016, *Facebook to Collect WhatsApp User Data, Violating FTC Order and Privacy Promises* (see https://epic.org/2016/08/facebook-to-collect-whatsapp-u.html).

139 Other sensitive issues may concern illegitimate agreements between undertakings or abuses of dominant position on the market, which are respectively regulated by articles 101 and 102 of the Treaty on the functioning of the European Union ("TFEU" – https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016E/TXT&from=EN). Article 101 sets out that *«1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between*

previously verify the feasibility of such mergers in view of their compliance with antitrust law. Nevertheless, in none of these cases antitrust authorities deemed necessary to stop mergers by reason of the market shares held by the buyer and by the purchased company. At any rate, the European Commission has recently levied Facebook with a 110 euro million fine for not having provided complete and correct information during the investigation phase since 2014. This information concerned the fact that Facebook was already able to automatedly match Facebook and WhatsApp users' accounts in 2014, but it declared the opposite to the European Commission when submitting its request for verification[140]. This did not have any impact on the decision allowing their merger, but the fine was however imposed because of the incompleteness of the information provided.

Although antitrust cases in the EU and in the US did not directly concern the protection or the availability of personal data by these undertakings, the investigations carried out are able to confirm that more and more interest is growing around such digital companies[141], because greater

Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which: (a) directly or indirectly fix purchase or selling prices or any other trading conditions; (b) limit or control production, markets, technical development, or investment; c) share markets or sources of supply; (d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage; (e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts. 2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void. 3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of: - any agreement or category of agreements between undertakings, - any decision or category of decisions by associations of undertakings, - any concerted practice or category of concerted practices, which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not: (a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives; (b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question». Article 102 TFEU reads as follows: *«Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist in: (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions; (b) limiting production, markets or technical development to the prejudice of consumers; (c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage; (d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts»*. For a detailed study on this articles, see J. F. BELLIS, I. VAN BAEL, *Il Diritto Comunitario della Concorrenza,* Turin, 2009; B. CORTESE, F. FERRARO, P. MANZINI, *Il Diritto antitrust dell'Unione europea,* Turin, 2014; B. CORTESE (ed.), *EU Competition Law. Between Public and Private Enforcement*, Amsterdam, 2013; F. GHEZZI, G. OLIVIERI, *Diritto Antitrust,* Turin, 2013.

140 See European Commission press release of 18 May 2017 (see http://europa.eu/rapid/press-release_IP-17-1369_en.htm).

141 On 19 December 2017, the German competition authority issued to Facebook its preliminary assessment on an alleged abuse of dominant position in the market sector of services provided by social networks and especially through infringements of data protection law, because the company collects data from users that surf third-party websites or apps thanks to an embedded application programming interface that is the so-called "Like-Button". Moreover, users are not aware of this huge collection of data and this is why the authority believes that they had not properly consented to the collection of their data (see the complete press release at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html). Besides, for instance, on 30 August 2018, Bloomberg announced that Google would have set an agreement with

concerns have been raised by the applicability of the EU GDPR in view of the extraterritoriality principle pointed out above. This regulation paves the way for a greater protection of personal data of users, consumers and individuals in general, that needs to be complied with also by these digital multinational holdings, usually been established under US law. However, despite being normally based in the United States, they are also used to setup subsidiaries in Europe for their own businesses. Notwithstanding this, the GDPR equally applies to them insofar as they have the said subsidiaries in the EU and they collect and process Europeans' personal information. Besides, the GDPR sets out detailed provisions for transborder data flows and for a better data subjects' protection. Yet, much has still to be done in terms of monitoring the implementation of the GDPR for EU public authorities, but also in terms of real compliance with it when it comes to controllers' and processors' duties.

Nonetheless, when considering the context of the – especially EU – digital market, as outlined in this paragraph, according to a vast majority of scholars and to the European Data Protection Supervisor, competition law could serve as another useful legal instrument to prevent companies from behaving in an illegitimate manner from the point of view of data protection law[142].

7. As outlined in the previous paragraphs, it can be stated that the rights to privacy and to data protection are closely connected to the right to human dignity.

This may be confirmed by the fact that the assignment (even for free) of one's personal data implies the exercise of one's self-determination in order to protect one's own intimacy and identity. Self-determination is a clear expression of human dignity, *i.e.* the need for the individual to have the full control of what he wants others to know about him. Once the individual founds himself limited in exercising his right to his informational self-determination, his consent to the collection and processing of his personal data may not be totally consciously given and his rights both to data protection and, accordingly, to human dignity, may turn out to be infringed.

Nevertheless, within the European Union, any of the said rights is currently protected as being fundamental and inviolable by virtue of the Charter of fundamental rights. This would mean

Mastercard, in order to verify if its users paying with the Mastercard system would have bought products or services that Google itself advertises to them, by analysing their credit card payment data released by Mastercard. (M. BERGEN, J. SURANE, *Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales*, 31 August 2018 – available at https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales).

142 F. COSTA CABRAL, *The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law,* cit.; F. COSTA CABRAL, O. LYNSKEY, *Family Ties: The Intersection between Data Protection and Competition in EU Law,* cit.; F. ZUIDERVEEN BORGESIUS, *Behavioural Sciences and the Regulation of Privacy on the Internet*, in A. ALEMANNO, A. SIBONI (eds.), *Nudge and the Law*, London, 2015, pp. 179-207; N. P. SCHEPP, A. WAMBACH, *On Big Data and Its Relevance for Market Power Assessment,* in *Journal of European Competition Law & Practice,* 2016, pp. 120-124; P. R. PRABHAKER, *Who owns the online consumer?*, in *Journal of Consumer Marketing,* 2000, pp. 158-171; R. PODSZUN, *The Digital Economy. Three Chances for Competition Law,* in *Maastricht Journal,* 2016, pp. 747-751; W. KERBER, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection,* retrieved from http://ssrn.com/abstract=2770479; J. KLEIN, P.M. RAO, *Competition and consumer protection in the cyberspace marketplace,* cit. See also EDPS, Preliminary opinion on *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy,* March 2014 (see https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf).

that, in principle, no other lower right or economic interest may overcome them. In practice, however, this does not always occur and both chronicle cases[143] and scholarly concerns demonstrate that personal data breaches are increasing, rather than being kept under control. This mostly happens because of the huge economic interests disguising behind the use of the web, which are even more fuelled by the flow and the availability of personal data allowing companies to have higher turnovers thanks to customised and targeted advertising activities, which let them save money that would otherwise be invested on market researches.

In view of the foregoing, not only are data protection laws important to safeguard data subject's moral integrity and dignity, but also competition law could come to the aid of consumers – who at the same time are individuals and data subjects – by ensuring that big companies do not make an illegitimate use of the massive amount of data they hold or of their market power, consequent to the availability of such data.

This paper focussed on a condensed comparative scrutiny between the European Union and the United States of America in terms of safeguard of dignity, protection of personal data and implementation of competition law in the digital market, by giving few hints on the issues arisen from the processing of personal data by US holding companies that should fall under the scope of the EU GDPR. The said processing raises concerns above all for EU citizens insofar as they feel being less protected under US data protection laws. And such a feeling might have been consolidated by some scholarly beliefs, based on the traditional theory of the supremacy of the EU over the US in the protection of fundamental rights.

Although it would be difficult to assess which one of the two legal systems would be better in this respect for the reasons outlined in the fourth paragraph, Baer's theory of the so-called «constitutional triangle» could be adopted in order to accept that different legal systems may recognise more importance to dignity and to the bundle of human rights connected thereto, alternatively to liberty and to the associated economic freedoms. Nevertheless, the greater relevance given to dignity or to liberty does not exclude the other from the triangle (together with equality), thus the two sets of values cannot be excluded one with another and must receive at least a minimum level of protection. This could be a reasonable explanation for different warranty levels in the EU and in the US. As a matter of fact, it cannot be said that the US do not protect human rights as the birth of the fundamental rights concerned in this paper are proved to be occurred thanks to American case-law and doctrine. Since EU competition law as well imitates the previous US antitrust model, the European Union may be said to have developed US legal traditions into more vigilant models. In an era where internet technologies are of everyday common use for professional or personal reasons and allow the entertainment of transnational relationships, in order to cope with personal data breaches, a wider multilateral approach would be preferred, both under data protection and competition laws. However, since it would not be easy to synchronise the activities

143 See, for instance, the recent datagate involving Facebook and a professor from Cambridge University, which let Cambridge Analytica have direct access to millions of Facebook users' personal data, so that the data mining company could combine and analyse data, in order to build political profiles of users around the world and try to persuade them in the exercise of their voting rights. See some of the many articles released on The Guardian and the New York Times at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far; https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

of EU and US privacy and antitrust enforcement authorities, because of considerable differences in their regulatory frameworks, much could be done by the same multinational companies, even by adopting – for instance – codes of conduct that would also increase their commercial reputation among consumers, by which they could grant adequate standards of protection for their consumers' personal data. In addition, they could also offer services and products designed in consideration of the most recent developments in privacy by design and privacy by default progresses, to make consumers feel more at ease with the technologies they use. Conversely, in the absence of a voluntary adaptation and compliance of at least the biggest firms, the European Union would reveal an added value when compared to the US legal system, by reason of its legal structure. As a matter of fact, at least the advantage of having harmonised data protection and competition laws for all Member States, as well as national and central enforcement separate authorities both for privacy and competition matters grants, it a more efficient approach in the protection of dignity and fundamental rights.

Outside its boundaries, the protection of EU citizens' dignity and data protection could be ensured thanks to the innovations brought by the GDPR, such as the extraterritoriality principle and the circumstance that, having recognised more rights relating to personal data, data subjects would be more aware of the risks to be avoided and of the remedies suitable to be employed for protecting their inviolable rights.

As the GDPR is applicable since a few months, scholars and case-law will be able to analyse its practical developments in the future and some precautions could still potentially be embedded in the proposal for the e-Privacy regulation, which is now under the scrutiny of the EU legislator.

FIORELLA DAL MONTE

I.3

Taxation and Big data: an analysis of the proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services (Proposal of the European Commission COM (2018) 148 final dated March 21, 2018)

SUMMARY: 1. Introduction. – 2. The digital economy and its main tax implication. – 3. The tax policy context. – 4. The Proposal of the European Commission. – 5. Some conclusive considerations.

1. According to one of its possible definition[144], big data are a «*high – volume, high velocity and / or high variety information assets that demand cost – effective innovative forms of information processing for enhanced insight, decision making and process optimization*».
Taking into account the link existing between big data and taxation, two main aspects are worth mentioning. On one hand, big data could represent a strategic asset for tax administrations, who are indeed data rich organizations. The data available to the fiscal authorities are traditionally those filed by the taxpayers themselves (through, for example, the tax returns) or, as an alternative, those collected directly by the tax authorities during their tax audits. In the current context, also thanks to the automated streams of information exchanged under initiative such as the Country – by – Country reporting, the tax authorities have at their disposal additional data, which, together with the traditional ones, are becoming big and thus representing an additional real – time set of information potentially enabling tax authorities to be more effective. The condition for the exploitation of such a potential key asset is the availability for tax administrations of big data processing technologies and the achievement of a high level of digital maturity[145].

On the other hand, the exploitation of big data represents one of the key features of the businesses active in the so called digital economy, about which the majority of the stakeholders take the view that the current international tax system is not able to properly capture the value created and, as a consequence, to tax it. In a nutshell, there is a quite common perception that some income produced by the digital economy is somehow «*stateless*»[146]. On such stateless income many jurisdictions would like to expand their taxing rights; the result is a very intense on – going debate, which is polarizing the interest of the international tax community.

Taking into consideration this second aspect of the big data, the paper focuses on the European Commission's directive proposal for the introduction of an *interim* digital service tax within the European Union[147] (hereinafter referred to as the "Proposal"), with the hope to give a

144 See https://www.gartner.com/it-glossary/big-data.
145 For an in – depth analysis of such an aspect, see OECD, *Technologies for better tax administration. A practical guide for revenue bodies*, Paris, 2016.
146 OECD / G20 BASE EROSION AND PROFIT SHIFTING PROJECT, *Addressing the tax challenges of the Digital Economy – Action 1: 2015 Final Report*, Paris, 2015, p. 12.
147 EUROPEAN COMMISSION, *Proposal for a Council directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services* (COM (2018) 148 final of 21.03.2018), available at http://eur-lex.europa.eu/.

contribution to the discussions that will take place next October within the first seminar organized by the University of Milan and entitled to «Big data and Law: new challenges beyond data protection».

At this aim, paragraph 2 of the paper gives an overview of the main characteristics of the digital economy – focusing in particular on the importance of big data – and the possible tax implications thereof. While these issues deserve an in – depth *ad hoc* study that is beyond the scope of the present paper, the analysis will limited to that preliminary considerations that are deemed necessary for a better understanding of the following parts. Paragraph 3 describes the current state of the debate, which is now on-going at the international, regional and national level, in order to make a complete reconstruction of the background behind the Proposal. A critical reading of the proposed directive is included in paragraph 4, with the intention of highlighting its significance and detecting possible areas of improvement. In this respect, it appears important to warn as from now the reader that all the available scholars' comments on the Proposal are quite negative[148]. In any case, the proposed directive appears to be of interest, since it represents the first tentative coming from a regional organization to introduce an unilateral interim tax measure to face the challenges posed by the digital economy. Some conclusive remarks are finally articulated in Paragraph 5.

2. As of today, there is no shared definition of digital economy; however, such a lack is quite understandable. On one hand, the digitalization represents indeed an extensive phenomenon, which encompasses all the businesses, with the consequence that «*the digital economy is increasingly becoming the economy itself*»[149]. In light of this aspect, scholarship has articulated the view according to which the term «*digitalization of the economy*» instead of «*digital economy*» would better apply to the current scenario. On the other hand, any tentative definition of the phenomenon under analysis is probably destined to become outdated in a short time, given the rapid development characterizing the digital economy. Having said that, the term «digital economy» is conventionally used in the context of this paper as a collective name making reference to a range of different activities, all of which have the following four salient characteristics in common[150].

148 J. BECKER, J. ENGLISH, *EU Digital Services Tax: a populist and flawed proposal*, in *Kluwer International Tax Blog* (March 2018), available at http://kluwertaxblog.com/2018/03/16/eu-digital-services-tax-populist-flawed-proposal/; CFE FISCAL COMMITTEE, *Opinion Statement FC 1/2018 on the European Commission Proposal of 21 March 2018 for a Council directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services*, in *European Taxation*, 2018, p. 371; A. M. JIMÈNEZ, *BEPS, the Digital(ized) Economy and the Taxation of Services and Royalties*, in *Intertax*, 2018, p. 635; L.A. SHEPPARD, *Digital permanent establishment and digital equalization taxes*, in *Bull. Intl. Taxn*., 2018; D. STEVANATO, *"Digital Tax" all'europea: una creatura deforme* (March 2018), available at https://www.leoniblog.it/2018/03/23/digital-tax-alleuropea-creatura-deforme-dario-stevanato/; A. TURRINA, *Which "Source Taxation" for the Digital Economy?*, in *Intertax*, 2018, p. 495; F. VAN HORZEN – A. VAN ESDONK, *Proposed 3% Digital Services Tax*, in *International Transfer Pricing Journal*, 2018, p. 267.

149 OECD, *Action 1 Final Report* (2015), *supra* n. 3, p. 11.

150 For the description provided in the present Paper, the position of the European Union has been mainly taken into consideration since the Paper focuses on the EU Commission's proposal and also because the position of the European Union is quite aligned to that of the OECD. More specifically, the OEDC lists the following aspects as key features of the digital economy: i) mobility with respect to intangibles, users and business functions, ii) reliance on «big data», iii) network effects, iv) use of multi-sided business models, v) tendency toward monopoly or oligopoly and vi) volatility due to low barriers to entry and rapidly evolving technology (see OECD, *Action 1 Final Report (2015)*, *supra* n. 3, at para. 4.3). In the more recent Interim Report published by the OECD, such aspects have been confirmed as key features

i) Limited physical presence of the businesses active in the digital economy, as a consequence of the decreased need for local personnel to perform business functions and the corresponding increased ability to conduct the business activity remotely (so – called «scale without mass» phenomenon). In other words, digital undertakings are able to manage their global operations on an integrated basis from a jurisdiction, which may differ from that / those jurisdictions in which the operations are carried out and the suppliers and customers are located.

ii) The importance of intangible assets which are crucial contributors of value for digitalized businesses. In this respect, it is worth underlining that the aforementioned feature of «mobility» applies also to the intangible assets on which the digital companies rely on, since the function of managing intangible assets can be assigned and transferred from one location to another (particularly within the same multinational group), with important consequences on where business' profits are subject to tax.

iii) Tendency toward monopoly or oligopoly, especially in case of immature markets where the company acting as first actor is usually able to achieve a dominant position in a very short time;
iv) Reliance on big data which are available to digital business thanks to the user participation. Data has always played an important role for businesses – also the traditional ones –; what characterizes the digital economy is the fact that data represent a component of the value creation process of such a relevance as never before: the use, collection and analysis of data is becoming an integral part of the digitalized business models. In order to better understand such consideration, it is important to further analyse the process – consisting of several phases – through which data become value. First of all, data have to be generated thanks to online activities performed by the digital services users; such data are stored and collected and, after a relatively short period of time, become big data, because of their increasing volumes. Big data are than processed, interpreted and analyzed: such step is essential in order to make the collected big data valuable; only through such analysis indeed, big data become readable and, as such, valuable.

According to a persuasive reconstructive study made by the OECD[151] – and taken into consideration also by the European Commission for the Proposal – , the involvement of the users in the phase of data origination characterizes all the business models of the digital economy. The level of such an involvement can instead vary from one business model to another. On one hand, the user participation is qualified as passive in all those cases in which the user does not perform any activity different to those strictly necessary in order to enjoy the online services (e.g. downloading an app, using a particular device or providing consent for user data to be collected). In all other cases, the user participation is qualified as active, even if with different possible levels. The lower level of user participation is required in case of recommendation mechanisms, involving activities such as bookmarking, tagging and rating, as it is typical for platforms providing for digital contents or IT solutions and e-commerce websites. An intermediary level of user participation characterizes instead activities such as writing comments and reviews (e.g. TripAdvisor) and taking and

of the digital economy, even if partially combined with each other. The result is a final list which includes the following aspects among the salient characteristics of the digital economy: i) cross – jurisdictional scale without mass, ii) reliance upon intangible assets (including intellectual property rights) and iii) data and user participation (see OECD / G20 BASE EROSION AND PROFIT SHIFTING PROJECT, *Tax Challenges Arising from Digitalisation – Interim Report*, Paris, 2018, at para 2.5).

151 OECD, *Interim Report (2018)*, *supra* n. 8, at para 143 – 149.

uploading photos and videos (e.g. Instagram and YouTube). The highest level of user participation is needed in case of social network (e.g. Facebook), in relation to which the user is asked to add friends and actively contribute to the creation of the community.

Moreover, also the way through which value is created from big data can differ from one digital business to another: several companies use directly the customer data collected for improving their own business operations while others monetize them by selling targeted online advertisements or, in any case, by transferring the user data to third parties.

Since the international tax rules currently in place have been established in the Twenties when the digital revolution was still far from happening, they disregard all the key features of the digital economy mentioned above. In very basic term, under the current international tax system, some sort of physical presence is required, being the permanent establishment the threshold for allocating any taxing right on the business profits of a non – resident company[152] to the market jurisdiction. However, as noted above, the business models of the digital economy are characterized by a limited physical presence: hence the major tension between the framework of reference provided by the international tax regime and the essential features of digital business models emerges. The result is the perception of the existence of what the scholarship has defined as a «*(digital) international tax gap*»[153].

3. The debate on how to fill such digital international tax gap dates back at least to 2013, when the OECD launched the 15 – point Action Plan on Base Erosion and Profit Shifting ("BEPS"). As part of such Action Plan, the OECD requested for public comments in relation to the tax challenges raised by digitalization. With the aim to be proactive in response to the OECD initiative, the European Commission set up a group of expert, assigning them the task to develop a comprehensive Union position on tax issues in the digital economy[154]. The outcome of the experts' work was included in a report[155], according to which, among the others, no special tax regime should be introduced for digital companies but any reform should have structured in general terms, with the introduction of simple, stable and predictable tax rules, the need of which has been strengthened by the digitalization.

In these years, the European Commission kept on working on the challenges of the digital economy, setting the creation of a Digital Single Market as one of its ten key priorities, with the aim of making Europe as world leader in the digital economy[156]. Direct taxation was deemed by the

152 The threshold of the permanent establishment is met in case that the non – resident company operates through a fixed place of business in a given jurisdiction or, as an alternative, through a dependent agent (the so called «agency permanent establishment»).

153 A. TURRINA, *Which "Source Taxation" for the Digital Economy?*, *supra* n. 6.

154 EUROPEAN COMMISSION, *Decision of 22.10.2013 setting up the Commission Expert Group on Taxation of the Digital Economy* (C (2013) 7082 final of 22.10.2013), available at http://eur-lex.europa.eu/.

155 COMMISSION EXPERT GROUP ON TAXATION OF THE DIGITAL ECONOMY, *Report*, 28.05.2014, available at http://eur-lex.europa.eu/.

156 EUROPEAN COMMISSION, *Communication to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe* (COM (2015) 192 final of 6.5.2015), available at http://eur-lex.europa.eu/. According to the definition provided by the European Commission, a «*digital single market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of*

European Commission to be one of the topics to be addressed – even if, at this stage, not the most important one – in order to make such a Digital Single Market concrete.

After 2 year – long work, the OECD issued in October 2015 a final report (Action 1) acknowledging that the digital economy exacerbates BEPS risks, as well as poses some challenges for the international taxation. The result was the adoption by the OECD of a «wait and see» approach, the main reason of which was the expectation that the anti – BEPS effects of other measures implemented within the BEPS project would have had a substantial impact not only on the BEPS issues, but also on the broader tax challenges posed by the digital economy.

As of today, such a position seems to be unviable: starting from 2017, the debate on digital economy has indeed further intensified both at international, EU and national level, suggesting that there is a quite common political pressure to act quickly. Without pretending to be exhaustive and starting from the international level, it should be mentioned that the G20 Finance Ministers requested the OECD to deliver a follow-up of Action 1. Hence, in September 2017, the OECD opened a public consultation, the outcome of which was an Interim report issued in March 2018[157]. In this occasion, the OECD takes a step forward if compared with the position expressed in BEPS Action 1: it acknowledges indeed that the tax challenges of the digital economy go beyond the boundaries of the BEPS concerns and address the redefinition of the criteria for the allocation of taxing rights on business profits among different jurisdictions. In this respect, the OECD states further that a consensus – based solution is needed for facing the challenges of the digital economy, that such kind of solution is not yet achievable since there are divergent views on how the issue should be approached and that, as a consequence, further work is needed, with the goal of producing an update in 2019 and a final report in 2020[158].

In this context, some countries have either adopted or announced the adoption of unilateral measures for the taxation of the digital activities: some examples are given by the so called diverted profit tax introduced by the United Kingdom, the equalization levy which applies in India and the web tax proposed by the Italian Government[159].

residence».

157 OECD, *Interim Report (2018)*, *supra* n. 8.

158 Just to mention the initiatives taken at the United Nations Level, the Committee of Experts on international cooperation in tax matters has issued a report entitled to the «*Tax Challenges in the Digitalized Economy*», with the aim to take a proactive approach in the on - going debate on the solution required for tackling the challenges of the digital economy, with particular attention to the needs of the developing countries (see UN COMMITTEE OF EXPERTS ON INTERNATIONAL COOPERATION IN TAX MATTERS, *Tax challenges in the digitalized economy. Selected issues for possible Committee Consideration*, 17 – 20.10.2017, available at www.un.org). Further work is expected to be done at the UN level. According to the recently released agenda of the next seventeenth session of the UN Committee of experts in international cooperation in tax matters to be held next October in Geneva, the tax consequences of the digitalized economy will represent one of the substantive issues to be discussed during the session (see UN COMMITTEE OF EXPERTS ON INTERNATIONAL COOPERATION IN TAX MATTERS, *Provisional agenda and organization of work*, 02.08.2018, available at http://www.un.org/esa/ffd/events/event/seventeenth-session-tax.html).

159 Italy appears to be at the forefront of the on – going debate on the taxation of the digital companies. A short term solution has been introduced by article 1, paras 1011–1019 of Law N. 205 of 27 December 2017 (Finance Bill 2018), with a deferred planned application starting from 1 January 2019. The objective scope of the proposed tax should be further specified by a decree issued by the Italian Ministry of Finance; such a decree – expected for April 2018 - has not been published yet. It is likely that Italy decide to prevent the entry into force of the measure, preferring to wait for the adoption of an interim tax at the European level. In this respect, see A. TOMASSINI, *L'incerta corsa alla tassazione*

I.3

At the intermediary regional level of the European Union, the importance of setting up a Digital Single Market has been remarked by the European Commission in May 2017[160]. In the following July, a discussion on the challenges of the taxation of profits of the digital economy was launched within the Council of the European Union. On September 2017 in the contest of his State of the Union speech, the President of the European Commission sent a letter of intent to the President of the European Parliament and the President of the European Council, announcing a legislative proposal establishing rules at EU level allowing taxation of profits generated by multinationals through the digital economy[161]. The Finance Ministers of Germany, France, Spain and Italy signed a joint political statement in support of EU law compatible and effective solutions «*based on the concept of establishing a so called equalization tax on the turnover generated in Europe by the digital companies*»[162]. At the informal ECOFIN meeting in Tallinn on 16 September 2017, six more member states expressed their interest and support to the approach suggested in the aforementioned joint political statement. In its communication entitled to «*A Fair and Efficient Tax System in the European Union for the Digital Single Market*» adopted on 21 September 2017[163], the Commission identified the challenges that the digital economy poses for existing tax rules and committed to analyze the policy options available. Following the Digital Summit in Tallinn on 29 September 2017, the European Council adopted on 19 October 2017 conclusion that underlined the «*need for an effective and fair taxation system fit for the digital area*»[164]. The ECOFIN Council conclusions of 5 December 2017 invited the Commission to adopt proposals responding to the challenges of taxing profits in the digital economy, highlighting the interest of many Member States for temporary measures, such as for example an equalization levy based on revenues from digital activities in the EU that would remain outside the scope of double tax conventions[165].

dell'economia digitale, in *Corriere Tributario*, 2018, p. 169. Besides, Italy has introduced a procedure of cooperation and enhanced collaboration that allows large multinational groups to discuss and examine jointly with the Italian tax authorities whether they may be deemed to have a permanent establishment in Italy (see art. 1*bis* of Law Decree No. 50 of 4 April 2017, converted by Law No. 96 of 21 June 2017). According to the intention of the Italian legislator, such measure is mainly targeted to companies active in the digital economy. For an in – depth analysis, see M. CERRATO, *La procedura di cooperazione e collaborazione rafforzata in materia di stabile organizzazione (c.d.* web tax *transitoria)*, in *Rivista di diritto tributario*, 2017, p. 751.

160 EUROPEAN COMMISSION, *Communication to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions on the Mid – Term Review on the implementation of the Digital Single Market Strategy. A connected Digital Single Market for all* (COM (2017) 228 final of 10.05.2017), in http://eur-lex.europa.eu/.

161 PRESIDENT OF THE EUROPEAN COMMISSION, *State of the Union 2017. Letter of intent to President Antonio Tajani and to Prime Minister Jüri Ratas*, 13.09.2017, available at http://www.un.org/esa/ffd/events/event/seventeenth-session-tax.html.

162 FINANCE MINISTERS OF FRANCE, GERMANY, ITALY AND SPAIN, *Political Statement. Joint initiative on the taxation of companies operating in the digital economy*, 07.09.2017, available at www.mef.gov.it.

163 EUROPEAN COMMISSION, *Communication to the European Parliament and the Council. A fair and efficient tax system in the European Union for the digital single market* (COM (2017) 547 final of 21.09.2017), available at http://eur-lex.europa.eu/.

164 EUROPEAN COUNCIL, *European Council meeting (19 October 2017) – Conclusions* (EUCO 14/17 of 19.10.2017), available at http://eur-lex.europa.eu/.

165 COUNCIL OF THE EUROPEAN UNION, *Outcome of the Council meeting. Economic and financial affairs* (15305/17 of 5.12.2017), available at http://eur-lex.europa.eu/.

4. The Proposal under analysis is the answer given by the European Commission to the aforementioned calls from several Member States of reacting quickly to the international tax gap: in this respect, the proposed introduction of a digital indirect service tax represents indeed a short – term solution, in order to face the current challenges of the digital economy. Alongside the Proposal, the European Commission has issued another legislative proposal (outside the scope of the present Paper) which constitutes the Commission's preferred long – term solution since it aims to reform corporate tax rules by introducing the concept of «*significant digital presence*»[166]. The distinction between the long – term and the short – term solution lies in the fact that only the former requires an amendment of the tax treaty framework currently in place (and, as a consequence, needs more time to be effectively implemented)[167].

The objective scope of the digital service tax is defined by article 3 of the Proposal, which qualifies as taxable revenues those resulting from the following services:

i) The placing on a digital interface of advertising targeted at users of that interface as well as the transmission of data collected about users and generated from users' activities on digital interfaces. The word «interface» is broadly interpreted by the Proposal (art. 2.3), in order to include any software, website or application that can be accessed by a user – both individual or business (art. 2.4 of the Proposal). By this way and making reference to the taxonomy included in the Impact Assessment[168], the proposed directive aims to tax all the fees resulting from those business models, in which access to a service (e.g. social network or search engine) is granted to users for free and personal data obtained from such users are than monetized by selling targeted advertisement placements or by selling the data itself to others businesses (e.g. Google and Facebook). In those cases where the supplier of the advertising service and the owner of the digital interface are different entities, only the former should be taxed, in order to prevent cases of double taxation (art. 3.3 of the Proposal).

ii) The making available to users of a multi-sided digital interface which allows users to find other users and to interact whit them, and which may also facilitate the provision of underlying supplies of goods or services directly between users (art. 3.1 b) of the Proposal). With reference to such kind of revenues, the Proposal aims to tax those fees paid by the users to access a platform, where the users offer services or goods among themselves (e.g. Airbnb or Blablacar). The revenues resulting from the supplies of goods and services made directly by the users connected thanks to the digital interface do not fall instead within the definition of taxable income according to the proposed Directive.

As expressly provided for in article 3.4.a of the Proposal, fees paid by users for accessing digital platforms which make available to them digital contents / IT solutions fall outside the scope

166 EUROPEAN COMMISSION, *Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence* (COM (2018) 147 final of 21.3.2018), available at http://eur-lex.europa.eu/. For an analysis, see R. PETRUZZI - V. KOUKOULIOTI, *The European Commission's Proposal on Corporate Taxation and Significant Digital Presence: A Preliminary Assessment*, in Eur. Taxn., 2018, p. 58.

167 In this respect, see A. TURRINA, *supra* n. 6, p. 502.

168 EUROPEAN COMMISSION, *Commission staff working document. Impact Assessment accompanying the documents "Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence" and "Proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services"* (SWD (2018) 81 final/2 of 21.3.2018), available at http://eur-lex.europa.eu/, Box 1 at p. 15.

of the Proposal (i.e. digital platforms providing media / content, gaming, electronic communication and payment services, cloud computing services and other digital solutions / software; in order to give some concrete examples, we can mention Netflix or Spotify). Further exemptions are provided for financial trading and crowd funding (art. 3.4.b – c of the Proposal). Also revenues related to distant sales model / e- commerce (Amazon) do not fall within the objective scope of the proposed digital service tax (preamble 13 of the Proposal).

In light of the above, it appears clear that the European Commission has opted for a targeted approach, selecting only some of the revenues resulting from the digital services. The reasoning of the European Commission underlying such selection appears quite articulate, even if it is not so clearly expressed in the Impact Assessment. Trying to build up all the logical steps, it appears correct to describe the reasoning of the European Commission as follows: the user participation contributes significantly to the creation of value for the digital businesses; such value is created in the user's jurisdiction and should be taxed there, according to the common shared «value creation» rationale which is a widely accepted principle pervading the whole BEPS project; however, under the current international tax rules, no taxing right is recognized to the user's jurisdiction because the services are provided remotely by the digital businesses with no physical presence in the market country or, in any case, with a very limited physical presence not meeting the permanent establishment threshold; in order to provide for a «*fair*» taxation – «fairness» is a recurring key word in the Proposal –, the best solution would be to implement a long term measure which would however require a global consensus – based solution and (probably) a coordinated amendment of the double tax treaties (and more time); but since there is a political imperative from some Member States to react quickly, a short term measure to be implementable within a reasonable time span is proposed, by selecting only those services «*where the participation of a user in a digital activity constitutes an essential input for the business carrying out that activity and which enable that business to obtain revenues therefrom*»[169], provided that they «*are responsible for the greatest difference between where profits are taxed and where value is created*»[170]. In other words, «[t]*he interim solution is meant to be a good and simple interim proxy to deal with the most extreme cases of mismatches between the location of taxation and value creation*»[171].

Taxpayers for the purposes of the digital service tax are all those legal entities[172] – irrespective of their tax residence –, which meet both of the following thresholds in a given year: i) a worldwide turnover exceeding Euro 750 million and ii) an amount of revenues subject to the digital service tax obtained within the European Union above Euro 50 million (art. 4 of the Proposal).

The first threshold (based on the total annual worldwide revenues) aims mainly to limit the application of the tax to companies of a certain scale, assuming that, as noted above[173], digital economy is characterized by big players taking the most advantage from the current digital

169 In this respect, see considerations made in paragraph 2 above.

170 EUROPEAN COMMISSION, *Explanatory memorandum of the Proposal*, *supra* n. 4, at para. 5.

171 EUROPEAN COMMISSION, *Impact Assessment*, *supra* n. 26, at para. 9.3.2, where further considerations of the European Commission are available.

172 Meaning any legal person or legal arrangement that carries on business through either a company or a structure transparent for tax purposes (art. 2.1 of the Proposal).

173 In this respect, see considerations made in paragraph 2 above.

international tax gap[174]. In this respect, the choice of the European Commission to set the same threshold as that provided for the country – by – country reporting[175] and for the common corporate tax base[176] appears positive, since it contributes to set up a coherent and easy framework in which market operators are required to take always the same threshold as reference for the applicability of a given tax regime / requirement. The second threshold aims instead, according to the European Commission's intentions[177], to limit the application of the digital service tax to those cases where there is a significant digital footprint at Union Level in relation to the revenues covered by the digital service tax.

The applicability of the digital service tax is extended by the Commission to both EU and non – EU entities, in order to make it compatible with the European Union law as well as with the International Trade Law. More specifically, with reference to the European Union primary law, the freedom to provide services (article 56 of the Treaty on the Functioning of the European Union ("TFEU")) implies the elimination of all discrimination on grounds of nationality, as well as the abolition of any restriction which is liable to prohibit, impede or render less attractive in concrete the activities of a foreign service provider[178]. At the international level, an analogous constraint is provided by article XVII of the General Agreement on Trade in Services, which prohibits a less favorable treatment of foreign service providers compared to the domestic one[179].

In this respect, some authors[180] have taken the view that the proposed digital service tax would in concrete address mainly non – EU (US) digital companies, determining a *de facto* discrimination for the foreign service providers. Such a conclusion seems to be confirmed by the data provided by the European Commission itself[181], according to which only a 7,2% share of the EU digital companies will meet both the thresholds set up by the European Commission.

Moreover, in a broader perspective, such an extension of the subjective scope of the digital service tax does not appear coeherent with the ultimate rationale of the tax under analysis, i.e. to tax fairly those entities who are non – resident within the European Union but create value there thanks to the European Union's users. In other words, because of the aforementioned comprehensive approach, the Proposal seems to go beyond its purposes, providing for the introduction of a new indirect tax also to entities which are assumed to be already fairly taxed, i.e. Member States tax resident entities, as well non – EU entities operating with a permanent establishment within the

174 EUROPEAN COMMISSION, *Explanatory memorandum*, *supra* n. 4, p. 10.

175 EUROPEAN COUNCIL, *Directive EU 2016/881 of 25 may 2016 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation*, available at http://eur-lex.europa.eu/.

176 EUROPEAN COMMISSION, *Proposal for a council directive on a common corporate tax base* (COM (2016) 685 final of 25.10.2016), available at http://eur-lex.europa.eu/.

177 EUROPEAN COMMISSION, *Explanatory memorandum*, *supra* n. 4, p. 10.

178 CJEU, Judgment of 22 October 2014, *Blanco and Fabretti*, joined cases C-344/13 and C-367/13, EU:C:2014:2311, available at http://curia.europa.eu/.

179 For an in – depth analysis (also with reference to the doubts of compatibility with the EU State aid law and VAT law), see N. BAMMENS, Y. BRAUNER, V. CHAND, R.J. DANON, L. DE BROE, P. PISTONE, L. SPINOSA AND A. TURRINA, *Request for input on work regarding the tax challenges of the digitalized economy* (October 2017), available at http://www.unil.ch/taxpolicy/.

180 J. BECKER, J. ENGLISH, *EU Digital Services Tax: a populist and flawed proposal*, *supra* n. 6; A. M. Jimènez, *BEPS, the Digital(ized) Economy and the Taxation of Services and Royalties*, *supra* n. 6; L.A. SHEPPARD, *Digital permanent establishment and digital equalization taxes*, *supra* n. 6, p. 2.

181 EUROPEAN COMMISSION, *Explanatory memorandum*, *supra* n. 4, p. 68.

European Union. This would lead to a situation of double taxation, about which the Proposal provides only for a deductibility of the digital service tax from the corporate tax basis[182].

As far as the place of taxation is concerned, those revenues deemed as taxable according to article 3 of the Proposal shall be treated as obtained in a member state if the user of the corresponding digital service is located in that Member State. In other word, the users create the connection between the taxpayer and the European Union. More in detail:

i) With reference to the placing on a digital interface of targeted advertising, the user shall be deemed to be located in a member state if the advertising in question appears on the user's device when the device is being used in that member state (article 5.2.a). In case of transmission of data collected about users and generated from users' activities on digital interfaces, the territorial condition is met if the data transmitted are those generated from the user while using a device in that member state (article 5.2,c).

ii) With reference to the multi – sided digital interfaces instead, a distinction is made if there is an underlying supply of services or goods between the users of the platform. If this is the case, the territorial requisite is met if the user uses a device in that Member State to access the digital interface and conclude the underlying transaction. Otherwise, the user shall be deemed to be located in a member state only if he has an account opened using a device in that Member State (article 5.2.b).

In this respect, the Proposal further clarifies that the Member state where a user's device is used shall be determined by reference to the Internet Protocol address of the device (art. 5.5 of the Proposal).

The provisions related to the place of taxation are probably the most interesting ones since their wording, as well as their structures appear totally new for the current tax system. Somehow such provisions disclose more than the others the European Commission's tentative (and the corresponding difficulty) to find adequate measures to fill the currently existing international tax gap.

The combined presence of the three aforementioned elements (i.e. taxable revenues obtained by a taxable person in a Member State) would make the proposed digital service tax applicable.
Moreover, from a practical point of view, this means that, in case that a digital business has (as it is quite likely to be) both EU and non – EU users, the share of revenues related to users non located within the European Union (and thus not covered by the digital service tax) should be firstly split from the total taxable revenues and then the remaining share of revenues should be apportioned within the Member States according to the several allocation keys laid down in article 5.3 of the Proposal for each type of taxable service. In case of businesses with users active only within the European Union, only the aforementioned second step should be implemented, in order to define the proportion of taxable revenues obtained in each Member State. Finally, in case of a pure domestic situation in which all the users of a digital business are located in the same member state, all the relevant revenues should be taxed there. Once determined the share of taxable revenues of each Member State in a given tax year, the digital service tax due in that member state shall be calculated applying the single rate of 3%.

182 See Recital 27 of the Proposal, which in any case represents only a recommendation to the Member States and not an obligation.

As far as the administrative aspects are concerned, a One – Stop – Shop simplification mechanism is provided by the Proposal: digital businesses can enjoy a single contact point, through which they can identify themselves for the purposes of the digital service tax, submit the relevant return and provide for the corresponding payments. A system of administrative cooperation should than allow the exchange of information as well as the transfer of the relevant payments between the member state of identification and the others where digital service tax is due (chapter 4 of the Proposal): by this way, a new requirement for administrative cooperation has been introduced within the current EU framework[183]. About such collection system, many doubts arise since it would probably share the same problem of the VAT one – stop – shop.

5. Being at the end of our critical reading of the Proposal, it seems appropriate to go back to the first line of the proposed directive, according to which its legal basis is article 113 of TFEU stating that the European Union is admitted to adopt «*provisions for the harmonisation of legislation concerning turnover taxes, excise duties and other forms of indirect taxation to the extent that such harmonisation is necessary to ensure the establishment and the functioning of the internal market and to avoid distortion of competition*». This means that, in order to recognize the competence of the European Union with reference to the Proposal, two conditions should be met. First of all, the digital service tax should be qualified as an indirect tax – as the European Commission does[184]. Moreover, the Proposal should be a necessary measure in order to eliminate, as far as possible, factors that may distort conditions of competition or hinder the free movement of goods and services, whether at the national or community level. Moreover, a special legislative procedure should be followed, which requires unanimity of all the Member States for the adoption of the Proposal. As of today, such unanimity appears quite difficult to be reached, also in light of the fact that the EU finance ministers were strongly divided upon the first discussion of the Proposal[185]. One could argue if, in case of absence of unanimity, the Member States in favor of the Commission's proposal (as Italy would be) could decide to introduce the *interim* measure by means of enhanced cooperation; however, also this root does not appear feasible since such a cooperation shall in any case not imply an undermining of the internal market, a barrier to trade between Member States, a distortion of the competition or a violation of the sovereignty of the other member states (see articles 326 – 327 of the TFEU). The result is that the adoption of the Proposal appears far from obvious, calling the European Union to keep on working on a global solution at the OECD level.

As it has been noted, «*in one way or another, it would seem that the existing body of international and supranational rules posing counter-limits on the adoption of unilateral measures are so pervasive that, were they to be eventually implemented, could actually appear as an*

183 For a reconstructive study of the framework currently provided at the European Union level with reference to the administrative cooperation in the field of taxation, see G. MARINO, *International and European measures for de – offshoring: global ambitions and local hypocrisies*, in *Intertax*, 2017, p. 530.

184 EUROPEAN COMMISSION, *Impact assessment*, supra 26. For a critical position of such qualification, see, among the others, A. TURRINA, *Which "Source Taxation" for the Digital Economy?*, *supra* 6.

185 See F. GUARASCIO, *EU digital tax on corporate turnover faces uphill road*, Reuters (28 Apr. 2018), available at https:// www.reuters.com/article/us-eu-ecofin-tax/eu-digital-tax-on-corporateturnover-faces-uphill-road-idUSKBN1HZ0JS.

equalization levy in name only or as a type of levy with fairly concerning distortive effects. Such a conundrum would seem to suggest that the current international legal framework appears more successful than anticipated in making international tax coordination unavoidable, virtually undermining the enactment of unilateral measures that would be in line with the policy objectives that have been outlined above»[186].

A final consideration should be articulated with reference to the item of the data protection, even if the seminar in occasion of which this Paper has been written aims to talk about the challenges arising from the use of the big data «*beyond data protection*». As mentioned above, the place of taxation for the purposes of the proposed digital service tax should be determined on the basis of the Internet Protocol address of the device of the users or, if more accurate, on the basis of other methods of geolocation. In this respect, the Proposal provides in generic terms that data should be collected for the purposes of the Proposal in a way that does not allow for the identification of the users (art. 5.6 of the Proposal). In addition to the above, recital 34 of the proposed Directive (even if not legal binding for the Member States) provides that any processing of personal data should be conducted in accordance with the EU Regulation 2016/679[187], with the further clarification that «[w]henever possible*, personal data should be rendered anonymous*» (emphasis added). The perception is that, at least in the field of taxation, the concerns about the right of the tax payers to protect their data still remain unanswered.

SILVIA SUT

186 A. TURRINA, *Which "Source Taxation" for the Digital Economy?*, *supra* 6, p. 519.

187 EUROPEAN PARLIAMENT AND COUNCIL, *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*, available at http://curia.europa.eu/.

.

I.4

Electoral freedom in the age of big data: an historical critique*

SUMMARY: 1. Introduction and methodological remarks. – 2. The origins and the meaning of electoral freedom. – 3. The regulation of media and mass media influence on the election. – 4. From electoral propaganda on the internet to the social media: what has changed in the relationship between electors and their representatives. – 5. Is electoral freedom truly jeopardized by the use of big data algorithms with political and electoral purposes? – 6. Conclusive remarks.

1. The recent and discussed case of Facebook - Cambridge Analytica had the result of giving a clear empirical evidence of how big data regulation may be relevant with respect to the democratic processes.

The scandal started in March 2018, after that the Guardian and the New York Times reported that a data analytics firm named Cambridge Analytica had harvested millions of users' data from Facebook profiles and used them to broadcast messages with political contents aimed at influencing electors political choices during the American Presidential Elections of 2016 and the Brexit Campaign in the UK, by virtue of the use of big data algorithms[188].

Such use of systems of data recollection explicitly addressed to broadcast political contents (often combined with the use of fake news[189]) to selected categories of electors, in order to meddle in political choices seems to have opened broad and multifaceted scenarios in the debate on electoral regulation and the protection of electoral freedoms.

In this perspective and in the attempt of underlining the most relevant aspects of the matter for constitutional law, we may indeed speculate on whether:

a) the meddling in public elections by virtue of the use of big data algorithms is a real new threat for the health of modern democracies;

b) the traditional paradigm of electoral freedom may be considered adequate before the increasing of external influence on election;

c) a new regulation of electoral meddling by virtue of big data algorithms is needed or the regulation of such phenomenon may be connected to the traditional legal discipline of media influence on the elections and / or political propaganda.

In order to correctly approach the above mentioned aspects, it is although necessary to clarify the definitions of the expressions «electoral freedom» and «big data».

188* Paper presented on 16th October 2018 during the Seminar «Big data and Public Law: new challenges beyond data protection» at Università di Milano.

It seems that the method allegedly used often implied the creation of fake social media profiles which were used to spread political contents and fake news about electoral competitors to selected categories of electors. See R. J. GONZALES, *Hacking the citizenry*? in *Anthropology today*, XXXIII, June 2017 and J. CARVALKO, *Defending against opaque algorithmic meddling in free elections*, in *Technology and society magazine*, June 2018, p. 30. For a more detailed outline on the case and the activity of Cambridge Analytica.

189 See with respect to the most recent works on the matter G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, 2017.

I.4

Electoral freedom is a well-known and broadly used basic constitutional concept, deeply rooted in the western liberal tradition since the XVIII Century revolutions[190].

For the sake of brevity[191] and in order to resume the key components of electoral freedom, it might be opportune to move from a simpler and more solid foundation, which might be actually offered by Article 21 of the Universal Declaration of Human Rights[192]. Indeed said article envisages the right to free and genuine elections and might be seen as a good synthesis of some of the most widespread and universally accepted principles of democratic processes.

Following the structure of Article 21, electoral freedom refers, on the one hand to the right of electors to express a free political choice without any external interference (genuineness of vote).

On the other hand, of course, electoral freedom is also referred to the need to ensure that any political competitor in the election may act in equal conditions (*par condicio* and equality of arms).

Finally, the guarantee of electoral freedom is also connected to the establishment of legal mechanisms of voting which ensure the realization of the above mentioned principles and also remedy to any possible distortion of same (guarantee of free voting procedures).

As per the definition of «big data algorithms» it might be useful to make reference to a well-known definition coined by anthropologist Justin Lane who describes big data as «*massive amounts of electronic data that are indexable and searchable by means of computational systems (...) stored in on servers and analyzed by algorithms*[193]*»*. Another important aspect we have to bear in mind is also the industrial dimension of the big data, as a market in which firms such as Facebook, Google and Twitter have the possibility of sharing and selling to third parties a huge amount of data harvested from their users[194].

Even though the use of big data with political purposes inspired a broad debate in legal doctrine[195], it appears that, somehow, the actual significance of many problems related to the impact of technological developments on fundamental processes of functioning of the State might be hard to evaluate with the eyes of a contemporary observer, as any historical phenomenon which is approximate in time.

In such perspective it might be opportune, indeed, to peruse the matter by virtue of an historical point of view, focusing the analysis on the progressive development of the principle of

190 See *ex multis* G. CHIARA, *Titolarità del voto e fondamenti costituzionali di libertà ed eguaglianza*, Milano, 2004; F. LANCHESTER, *Voto (diritto di)*, in *Enclicopedia del diritto*, XLVI, Milano, 1993; G. SCHEPIS, *Elezioni (storia dei sistemi elettorali in Italia*), in *Enciclopedia del diritto,* XIV, 1965.

191 Clearly a complete analysis of the issue should require a deeper effort which is inconsistent with the aim of the present paper.

192 «*Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. Everyone has the right to equal access to public service in his country. The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures»*.

193 J. E. LANE, *Big data and anthropology: concerns for data collection in a new research context*, in *Journal of the Anthropological Society of Oxford-online*, January 2016, p. 74.

194 See J. E. LANE, cit., p. 74-88.

195 See G. BELL, *The secret life of big data*, in T. BOELLSTORFF, B. MAUER (eds.), *Data now bigger and better*, 2015, Chicago, p. 7-26; V. M. SCHONBERGER, K. CUKIER, *Big Data: a revolution that will transform how we live, work and think,* Boston, 2013.

electoral freedom and correspondent legal regulation of the external influences on elections, with special reference to the influences of the media.

Hence the paper, moving from the above mentioned theoretical and methodological premises, aims at giving some brief conclusions on the possible intersections of electoral freedom and the use of big data algorithms to orientate political choices in the light of the historical roots of the principle of electoral freedom and the various examples of the regulation of external influences on national elections. Moreover it will be also necessary to speculate on whether the problem of the misuse of big data algorithms with the purpose of meddling in the elections shall be considered as a real and new threat for electoral freedom and electoral systems or it might be treated as another chapter in the evolution of legal regulation of mass medias influence on electoral processes.

2. We can easily affirm that the concept of electoral freedom[196] truly represents one of the key and basic principles of modern democracies[197]. Such principle indeed, in its first meaning, has been originally designated with reference to the need of protecting electors from any possible improper influence and limitation that could jeopardize the genuineness of their political choice.

Under this point of view it is possible to read all of the traditional guarantees of electoral rights such as the secrecy of vote, which was perceived, since the French Revolution, as the most important defense for the new electors[198].

Notably the French Revolution with its rupture with the *Ancien Régime* represented a key moment for the debate on electoral systems design as well as the perfect «*humus*» for the raise of the public theories on the set of warranties that have to be ensured in order to pursue the guarantee of electoral freedom during the elections[199].

Under a different point of view, the concept of electoral freedom was also intimately linked to the idea of universal suffrage. On the one hand, as affirmed by Huard, «*il y a suffrage universel quand aucune condition d'âge autre que la majorité légale et aucune condition financière n'est imposée pour participer au scrutin*[200]». In other words, in order to actually achieve universal suffrage it is

196 Hereinafter the reference to electoral freedom must be interpreted as inclusive of the set of principles envisaged under Article 21 i.e. genuineness of vote, equal access to elections, and fairness and freedom of the voting procedures (see *supra* p. 2).

197 With respect to the close relationship between electoral freedom and democracy see H. KELSEN, *I Fondamenti della democrazia* (1929), Bologna 1966; N. BOBBIO, *Il futuro della democrazia*, Torino, 1995; M. LUCIANI, *Il voto e la democrazia*, Roma, 1991.

198 Nevertheless it is opportune to mention some relevant opinions of important authors of the age such as J. J. Rousseau, who believed that the secrecy of vote may also lead to the diffusion of the corruption in the public offices in particular if accompanied by the lack of efficient instrument of prevention of the abuses. The lack of secrecy anyhow is also strictly connected with the idea of vote as a public function, involving a view of the voter as a citizen who is performing a constitutional function instead of a simple individual (see the following footnote).

199 Notably, since the French Revolutionary Convention of 1792, the right to vote has been indicated properly as a *droit* (i.e. individual right), and by virtue of such nature it had to be accompanied by a set of warranties aimed at ensuring that it could be freely exercised by the citizens. The opposite model that envisages the vote as a *fonction*, i.e. a public function, laid the foundation for the raise of systems of restricted suffrage based on minimum wage or capacity of the electors (e.g. in reading and writing).

200 R. HUARD, *Le suffrage universel en France (1848-1946)*, Paris, 1991, p. 25, reported by M. ROSPI, *La tutela della segretezza del voto e l'evoluzione della democrazia. Uno studio di diritto comparato*, IV seminario annuale del Gruppo di Pisa, Università Roma Tre, 18 September 2015 available at www.gruppodipisa.it.

mandatory to ensure that no conditions are envisaged in order to grant the right to vote to the electors[201].

On the other hand, universal suffrage could only be achieved if the electors could count on the fact that they were able to vote in the lack of external pressure and consequences due to the choices expressed.

In this respect, the set of warranties linked to the right to vote such as the secrecy of vote[202], the lack of burdens of age[203] and wage that we can connect to electoral freedom, had to be considered as necessary also in order to achieve the universal suffrage[204]. Hence, their protection truly represented, under such perspective, a basic constitutional objective.

Nonetheless, the contradictory relationship between universal suffrage and the provision of conditions of wage and capacity to have access to elections represented a typical feature in the debate on electoral rights in the centuries XVIII and XIX[205]. The actual realization of the revolutionary principle of equality was in fact hindered by a bourgeois ruling class with oligarchic and homogeneous purposes which was interested in maintaining the control of society[206]. Said contradiction progressively disappeared with the effective extension of suffrage and the crystallization of the principles addressed to guarantee electoral freedom, in general terms, from the first decades of the twentieth century.

The centrality of the principle of electoral freedom for modern democracies is, as we said, well known and commonly accepted within constitutional doctrine. As per the Italian constitutional experience, such centrality[207] is also well testified in the Preparatory Papers of the Italian Constitutional Assembly, in which it has been defined as an «objective liberty of exercising the right to vote for the benefit of electors that the authorities of the State have the task to ensure[208]». In this respect, while it is clear that public authorities have to ensure the lack of illegitimate pressure and influences on electors, it is opportune to point out that another significant issue connected to electoral freedom is actually the identification of those influences that might be considered as legitimate[209].

The prior interest of the legislator in such respect is clearly to avoid those influences that may jeopardize the free and genuine expression of voter's choice as well as punishing those attempts of interventions aimed at interfere in the suffrage[210].

201 See E. BETTINELLI, *Diritto di voto*, in *Digesto - Discipline pubblicistiche*, Torino, 1990, p. 7.
202 The principle was also included in the French Constitution of 1795.
203 Except for legal age envisaged for the access to vote.
204 Notably in the lack of such guarantees many electors could have been forced to renounce to their right to vote due to the concerns on the consequences of the votes expressed.
205 See M. S. GIANNINI, *Il pubblico potere*, Bologna, 1986; C. MORTATI, *Le forme di governo. Lezioni*, Padova, 1973.
206 F. LANCHESTER, *Stato (forme di)*, in *Enciclopedia del Diritto*, Milano, XLIII, p. 803.
207 See in such perspective C. LAVAGNA, *Istituzioni di diritto pubblico*, Torino, 1985, p. 525; L. PALADIN, *Diritto costituzionale*, Padova,1991, p. 292. Said authors make reference to electorate freedom as the most significant and general feature of the suffrage.
208 Free translation of the declaration made by Umberto Merlin. See *Atti dell'Assemblea costituente*, II, Roma, 1951.
209 See. F. LANCHESTER, *Voto (diritto di)*, in *Enciclopedia del diritto*, XLVI, Milano, 1993, p. 8.
210 It is properly the area of intervention of the electoral felonies which under Italian law are mainly regulated by the Statute no. 61/2004.

Finally another public interest connected to the guarantee of electoral freedom, as we said, is the need of avoiding that some particular political forces may illegitimately benefit from undue advantages on other political parties. It is indeed the dimension of electoral freedom to which we referred in terms of guarantee of the fairness of the electoral competition or *par condicio* and it is basically the main ground in which we may move the debate on big data influences on elections.

In this respect, legal doctrine agrees in individuating in the preparatory phase to elections a key moment for the actual guarantee of electoral freedom, both on the side of genuineness of the choice of voters and the fairness of the electoral competition[211].

The regulation of electoral propaganda (i.e. the activity that political bodies carry on in order to convince the subjects entitled to vote[212]) is, in such perspective, one the of the most important concerns of the legislators with respect to the purpose of avoiding information asymmetries and ensuring a more conscious choice for the electors.

In order to carry on our analysis it is then opportune to dwell on the subject of the historical evolution of the regulation on political propaganda. Such reconstruction, however, has to consider that in those legal systems inspired to the principle of free elections, electoral propaganda has to be seen both as a fundamental liberty as per political entities rights as well as a possible threat to the rights of voters also subject to constitutional protection[213].

3. The history of the regulation of political propaganda may be linked, for our purposes, to the history of the technological development of the media and the mass media and their use to broadcast political contents aimed at convincing the electors to take a particular political decision.

Clearly the media have always existed but it is basically from the XX Century that they have reached a communicative capacity such as to be denominated as mass media[214].

Radio and television have led to a new and broader connection between audience and broadcasters of contents including, of course, messages with political and electoral purposes.

The potentiality of the new mass media and their possible use in order to influence the course of elections was immediately clear also to the different legislators with respect to the regulation of electoral propaganda.

In general terms, as anticipated in the former paragraph, the regulation of political and electoral propaganda[215] is basically focused on the goal of avoiding illegitimate influences on the election as well as ensuring the effectiveness of the principle of the equality of arms, which would

211 See E. FERRIOLI, *La disciplina delle campagne elettorali e referendarie*, in R. NANIA, P. RIDOLA, *I diritti costituzionali*, Torino, 2001, p. 623; S. BAGNI, *La propaganda elettorale tramite internet: quale disciplina*, in *Dir. informatica*, I, 2004, p. 634. Another term which is commonly used in legal doctrine in this respect is «equality of chances» of any participant to the electoral competition. Said expression clearly shows the link between electoral freedom and the constitutional principle of equality.

212 See F. LANCHESTER, *Propaganda elettorale*, in *Enclicopedia del diritto*, XXXVII, Milano, 1988.

213 F. LANCHESTER, *Propaganda elettorale*, cit., p. 8.

214 See for further remarks on the topic R. BIANCO, *Diritto delle comunicazioni di massa*, 2007, Bari. See also G. BUSINO, *Propaganda*, in *Enciclopedia Einaudi*, Torino, 1980 for a broader historical reconstruction. According to the latter indeed the real origins of propaganda have to be found as well during the French Revolution in which for the first time such phenomenon became a stable and developed component of political competition.

215 For a definition of such expressions see E. BETTINELLI, *Propaganda*, in *Digesto - Discipline pubblicistiche*, Torino, 1997.

be violated if a political body may count on a particular advantage on competitors provided by the control of the mass media[216].

However, since political propaganda represents a fundamental right directly linked to the right to free expression, the legal discipline of electoral propaganda has to ensure that such liberty is balanced with the above mentioned principles connected to electoral freedom[217].

In this respect, as per Italian regulation of the matter[218], it is possible to affirm that such balance has been pursued according to two different types of regulation linked to the different stages of the electoral process[219].

The first type of regulation refers to the last phase of the election and basically consists in the provision of a period of electoral silence aimed at granting the electors a short period to process the electoral choice without further direct influences by political competitors.

The second type of regulation deals with the need of ensuring the *par condicio* of political competitors that is granting all the participants the same chances in terms of use of mass media to broadcast political contents. Such exigence is indeed pursued by virtue of the provision of time limitations for the broadcast of electoral spots on radio and television as well as the introduction of a maximum number of political messages per day[220].

With reference to the above mentioned profiles, the main stages of the regulation on media influence on elections in Italy may be individuated as follows: as per the so-called electoral silence, the Italian statute no. 212/1956[221] had already established a legal discipline of electoral propaganda and political communication which envisaged some rules on the use of campaign advertisement and posters during the 30 days before the elections and introduced at Article 9[222] the so-called electoral silence[223] during the day before the elections and the day of the vote[224].

Notably, such discipline was not applicable to electoral propaganda on radio and television, with the consequence of an important gap in the regulation of propaganda. Only in 1975[225] with the

216 See F. LANCHESTER, *Propaganda elettorale*, cit., p. 9.

217 The opinion is also confirmed by the jurisprudence of the Italian Constitutional Court that affirmed the need of protecting the liberty of choice of electors, who have the right to express their political opinion rationally. In this respect, the Court stated that the persuasive strength of television (also with respect to the other mass media) may jeopardize the free capacity of choice of the electors because of its pervasive nature. Said characteristics, according to the Court, shall therefore justify a strict regulation of the use of the television to broadcast political contents (see *ex multis* Constitutional Court no. 48/1964, 225/1974 and 148/1981).

218 For sake of brevity the paper focuses on the evolution of the legal discipline of the matter under Italian law but many of the remarks may be extended to other legal systems.

219 See S. BAGNI, cit., p. 633.

220 Cf. S. BAGNI, cit., p. 634.

221 Named «*Norme per la disciplina della campagna elettorale*».

222 Which has been deeply modified by Article 8 of the Statute no. n. 130/1975.

223 During the electoral silence it is forbidden to carry on campaign speeches and electoral caucuses as well as organizing any form of political propaganda within 200 meters from the places in which the voting operation will be held.

224 In general terms, with respect to the electoral silence, see G. MAZZOLENI, *La comunicazione politica alla vigilia della seconda Repubblica*, in *Problemi dell'informazione*, 1993, from p. 212.

225 Between those regulations it is opportune to make reference to the important decision of the Italian Constitutional Court no. 48/1964 in which the Court stated that the limitations to political propaganda were in line with the provisions of the Constitution and, moreover, such limitations do not affect freedom of speech and have to be referred to the principle of the *par condicio* and / or equality of chances which has also a constitutional foundation. See F.

Statute no. 103/1975 a first (and probably incomplete[226]) regulation of the matter has been achieved[227].

Another important step in the evolution of the regulation of political propaganda may be seen in the approval of the Statute no. 515/1993[228] which was inspired by the purpose of providing a general and organic discipline propaganda (in all of its forms)[229] including specific rules on acquisition and access to the press[230], the other mass media as well as mechanisms of public audit[231]. Even though the Statute represented an important stage in the progressive regulation on propaganda on the media, soon it became clear that the provisions included therein were unsuitable for an effective guarantee of the *par condicio* and the genuineness of vote. Hence, some significant amendments were introduced by the Legal Decree no. 83/1995[232] and finally by the Statute no. 28/2000.

Such Statute has represented a new kind of approach to the regulation of propaganda since it envisaged a set of rules which were applicable to all electoral campaigns and political communications for the whole year[233]. Basic principles of the new regulation, according to Article 1 of the Statute were indeed: the guarantee of the *par condicio* and impartiality with respect to all political subjects, the promotion of the free access to the media for political communication and the regulation of the use of the media during electoral campaigns[234].

Finally, as per the last examples of political propaganda and use of mass media it is opportune to mention the Statute no. 313/2003 which included a set of provisions finalized to ensure the *par condicio* with respect to local radio and TV broadcasters, and the Statute no. 215/2012. The latter has amended the Statute no. 28/2000 with the introduction of provision aimed at promoting *par condicio* in terms of gender representation with reference to the access to mass media propaganda[235].

LANCHESTER, *Propaganda*, cit., especially the footnote 58, for further remarks on the case and its impact on Italian regulation of propaganda.

226 See C. CHIOLA, *Disciplina della propaganda elettorale delle emittenti private*, in *Il diritto delle radiodiffusioni e delle telecomunicazioni*, Milano, 1984, p. 2.

227 The Statute also insituted a parlamentary commission (Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi), also known as Commissione di Vigilanza Rai with functions related to the audit of the national television and radio services and regulation of *par condicio* and political propaganda.

228 Named «Disciplina delle campagne elettorali per l'elezione alla Camera dei deputati e al Senato della Repubblica».

229 See R. BORRELLO, *Stampa e par condicio: riflessioni critiche sulla vigente disciplina*, in *Giur. cost*., 3, 2008, p. 2769.

230 An important measure included under the Statute was the prohibition for the press to publish electoral previsions and statistics on electoral intentions within the 15 days before the elections.

231 Article 2 of the Statute included for instance the prohibition during the 30 days before the elections to broadcast all forms of messages of political propaganda on newspapers, television and radio with the exception of those political contents that ensured the realization of the *par condicio* principle such as political debates, conferences and other events with the presence of political competitors. Said Article would have been repealed by Statute no. 28/2000.

232 Also commonly named as «Decree Gambino».

233 Not only with respect to the period before the elections.

234 For a more detailed review on the Statute see R. BORRELLO, *Oggetti politici e trasmissioni radiotelevisive: prime riflessioni comparatistiche sulla legge n. 28 del 2000*, in *Giur. cost*., 1, 2000, p. 635.

235 See R. BORRELLO, *Stampa e par condicio: riflessioni critiche sulla vigente disciplina*, in *Giur. cost*., 3, 2008, p. 2769.

4. The diffusion of the internet and its use to broadcast political and electoral messages addressed to users truly represented a sort of revolution in the debate on the regulation of influences on electors and freedom of vote[236].

Since the second half of the nineties political parties massively used internet as a tool for electoral propaganda[237], even in the lack of a relevant regulation of the matter. As per Italian legal system indeed, neither the above mentioned Statute no. 28/2000 nor the most recent measures adopted, such as the Legislative Decree no. 44 del 2010[238], have provided an organic legal discipline of the electoral propaganda on the internet[239].

Notwithstanding the above remarks, it is opportune to add that in some cases a partial regulation of single aspects of the matter has been achieved by virtue of several rulings issued by the Italian Data Protection Authority especially with reference to the use of massive email-spamming of political contents to users in the imminence of the elections.

In such concern, since the 2005 the Authority has been affirmed some important principles related to the broadcast of political messages directed to influence the electorate by email, sms, fax to electors, affirming the need of a previous and explicit consent of voters as well as the disclosure of the privacy policy of the broadcaster[240].

Moreover, another aspect which is worth pointing out is the difficulty of legislators to adapt to the internet revolution the traditional principles on *par condicio* in the use of communicative tools for the political bodies and genuineness of vote. It is self-evident indeed that on the one hand, the traditional legal solutions such as electoral silence and limitation of broadcasting of political messages are hardly applicable to the internet in the age of the so-called «e-democracy[241]». On the other hand, due to the deep differences between the internet and the traditional mass media, the regulation of the latter is as well hardly subject to an extension to the political propaganda on the internet.

The delay and the difficulties of the legal regulation of propaganda on the internet has been confirmed also by the critical issue of the increasing use of social networks to broadcast political contents to users and in general as a basic tool of modern political communication.

The topic of the diffusion of the social networks and their use to pursue political goals, however, offers the chance to reflect on a broader issue, which seems to be critical also in order to duly approach the matter of the use of big data algorithms to meddle in the elections.

236 See *ex multis* A. VALASTRO, *Internet e strumenti partecipativi nel rapporto tra privati e amministrazioni*, in M. NISTICÒ, P. PASSAGLIA (eds.), *Internet e Costituzione*, Torino, 2014; S. RODOTÀ, *Tecnopolitica*, Bari-Roma, 1997.

237 See S. BAGNI, *cit*., p. 629 who refers to the broad use of internet since the campaign for the elections of 2004 in Italy.

238 Which included the definition of media audiovisive services that, however, is not applicable to internet websites.

239 As it has been observed by P. COSTANZO, *Quale partecipazione politica attraverso le nuove tecnologie comunicative in Italia*, in *Dir. informatica*, I, 2011, p. 21.

240 See *ex multis* the so-called «Authority's Prescriptions» ex Article 154, par. 1 of the Legislative Decree no. 196 del 2003 dated 11.02.2010 and the relevant considerations in P. COSTANZO, *Quale partecipazione politica attraverso le nuove tecnologie comunicative in Italia*, cit., p. 23. With respect to the most recent documents adopted by the Authority, see «Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall´informativa per fini di propaganda elettorale» dated 6th March 2014.

241 See for a more detailed analysis of the issue P. COSTANZO, *Profili costituzionali di internet*, in E. TOSI (eds.), *I problemi giuridici di internet. Dall'E-commerce all'E-Business*, Milano, 2003, p. 89.

In this respect, indeed, the matter deals with one well-known topic in current constitutional debate on political parties and technological development: internet does not simply represent a new tool to communicate but it has deeply changed the basis of the democratic relationship between the electors, their representatives and intermediate bodies such as political parties[242].

If it is true that, on the one hand, internet has provided the political bodies with a powerful tool to influence voter's opinions, it is opportune to remark that, on the other hand, with the use of the internet and the social networks the electors have found a way to directly connect with their representatives and gained several new methods of participation in the democratic processes[243].

In other words internet has deeply impacted democracy in a variety of ways and it seems that, regardless of our efforts, it is impossible to reconnect the previous changes in mass media evolution from newspapers to the radio and from the radio to the television[244] to the internet revolution.

5. It appears that the use of big data algorithms to meddle in the elections and influence key portions of the electorate has to be perused bearing in mind the above mentioned premises and remarks, with respect to the ongoing revolution of democratic relationship that internet and social network have triggered.

The brief review of the historical evolution of the regulation of external influences on elections demonstrated that the main aims of legislator connected to electoral freedom were focused on realizing *par condicio* / equality of arms of political competitors and protecting the genuineness of vote, basically with the selection of those influences that could be considered inadmissible and / or illegal.

In this respect we have firstly to speculate on whether the big data phenomenon, as shown in the Facebook – Cambridge Analytica case, may truly have a serious impact on the above mentioned principles and, in the positive, what can legislators do in order to prevent the violations of same.
As per the realization of *par condicio* between political competitors, it seems that even the massive forwarding of political contents by virtue of the use of big data algorithms, does not entail particular problems as long as all electoral competitors may have access to the tool. It is the case of the appointment of data analytics firms like Cambridge Analytica that have been working on behalf of political bodies since quiet long time[245].

In such perspective indeed the use of internet and big data algorithms may simply be seen as another example of technological development of electoral propaganda, that does not impact, in standard conditions (i.e. when all actors have the same possibility of access) on electoral freedom.

242 The literature on the matter is abundant. See T. E. FROSINI, *Internet e democrazia*, in *Dir. Informatica*, 2017, p. 657; P. MARSOCCI, *Lo spazio di Internet nel costituzionalismo*, in *Costituzionalismo.it*; U. ALLEGRETTI, *Democrazia partecipativa*, in *Enc. dir.*, 2011, p. 295.

243 Notably internet helped in achieving transparency as it has also provided electors with the tools to verify the information provided by their representatives.

244 See M. BASSINI. *Partiti, tecnologie e crisi della rappresentanza democratica. Brevi osservazioni introduttive*, in *Diritto pubblico comparato ed europeo*, 2015, p. 867.

245 See J. NAUGHTON, *Us Elections 2012: is Facebook the "Real Presidential Swing State"?*, in *Observer*, 2, September 2012 who explains how even during the 2012 Presidential Elections in the US, the Democratic Party has invested a huge amount of money aimed at set up a program of targeted propaganda and user's data analysis on social media, also with the help of specialized firms.

Of course the guarantee of equal access represents a basic condition in such perspective and shall be treated within the debate on transparency and impartiality of the internet, which however does not fall within the object of the present article[246].

The impact of big data algorithms used with electoral purposes on the genuineness of the vote on the other hand, seems to have opened more complex issues. Firstly, also in this case we can argue that the attempt of influencing electors with various means does not represent a novelty in the history of democracy. Hence, as we said, under such point of view we are simply dealing with a more accurate example of technological improvement of those means of influence.

Nevertheless the issue seems to be more complicated especially when approached in connection with the broader debate on the on-going challenges that the social networks and the internet have brought with respect to the traditional guarantees of electoral freedom, particularly the secrecy of vote. The number of available information of electors, indeed, has reached severe dimensions and such amount of data may have a direct impact also with reference to the electoral process. Notably several companies have developed complex algorithms capable to elaborate accurate previsions, also in terms of opinions and political preferences, just requiring a relatively small number of user's information.

On the other hand we also have to point out that in many cases it is the same population of the social networks that agrees to express and share political opinions on the internet (e.g. comments on blog or media website, inscription to groups on social media). This disclosure clearly has the effect of providing precious and useful information for big data analysts (and hence for the political bodies that hire their services) and often produces the effect of affecting the secrecy of vote.

In such perspective we also could remark that some of the traditional guarantees of freedom of vote such as the same secrecy, which were designed within an oligarchic society with a significant distance between representatives and the electoral bodies, seem to need now to be adjusted to the current status of electoral competition. Of course this does not mean that such guarantees are useless. On the contrary, it has to be enhanced with respect to the current problems that we are facing nowadays.

In other words the right of expression, which includes the right to express of political opinions using a social network, has to be protected with a set of measures pursuing electoral freedom that should also prevent the misuse of user's information to possibly influence the electors. In this concern, indeed, it seems that it is within the protection of personal data of internet users that we should study the issue of the modern regulation of genuineness of vote, with the purpose of condemning the illegitimate harvesting of data and other violations that may help in providing information that could be used for political profiling or with the purpose of meddling in the elections[247].

In such respect, however, we have to point out that, as noticed in the previous historical reconstruction, the protection of the genuineness of electors choice has been always achieved with a

246 With reference to the matter see P. COSTANZO, *Quali garanzie costituzionali per gli interventi rimediali in rete*, in *Dir. Informatica*, 2013, p. 17; C. ROSSELLO, *La governance di internet tra diritto statuale, autodisciplina, soft law e lex mercatoria* in *Dir. comm. internaz*., 2006, 1, p. 45.

247 However it is opportune to point out that it is not possible to do much in those cases in which the sharing of personal information and opinions correspond to the consent and the free will of the users.

selection of those influences that could be considered as illicit. Thus, modern legal regulation aimed at protecting electoral freedom should probably focus mainly on the persecution of illicit methods of data collection, breaches in users privacy[248] and cyber-attacks during elections instead of attempting to regulate the thousands of possible factors of influence on electors that may come from internet, social network and big data algorithms.

6. The case of Cambridge Analytica seems to have put in light how big data algorithms may be used with political purposes and possibly in the attempt of meddling in the elections. Nevertheless many authors seriously doubt about the effective benefits of the use of such tools for the political campaigns[249].

However for the reasons indicated in the present papers it seems it is possible to affirm that we are actually facing a new stage in the evolution of technological tools applied to electoral propaganda.

Nevertheless, as we have said, the phenomenon has to be also studied with reference to the profound changes that have affected the relationship between electors and their representatives due to the raise of the internet and the social network and their use in the democratic processes.

It seems indeed that the very same concept of electoral freedom has changed in view of the current and different needs of the electors that legislators have to fulfil with the adoption of a suitable legal regulation. In this concern it appears that the most urgent needs of electors linked to the promotion of «modern electoral freedom» deal with the protection of personal data and privacy of the users on the internet.

Hence when we try to speculate on possible legal measures to adopt in such purpose it is probably in the above mentioned areas that an actual intervention of legislators is needed.
On the other hand, other useful legal tools may be represented by the regulation of political parties misconducts involving the use of data harvested with methods lacking in transparency.

It is the case of the amendment that the EU Commission is currently drafting to EU party funding rules with the purpose of imposing fines on political parties who misuse personal data of the electors to carry on their campaigns[250]. The measure is supposed to be applicable to the parties

248 Making reference to legal evolution of the matter in Italy it is interesting to remark that even with regards to electoral propaganda by email and sms from 2005 the first important contribution in the development of regulation was provided by the Italian Data Protection Authority on the ground of privacy and protection from data breaches instead of the ground of regulation of political propaganda *tout court*. Under such point of view the current *status* of legal regulation, with the lack of a discipline of electoral propaganda carried out with the use of big data and social network has several common elements with the above mentioned period. Hence maybe the legal solution adopted in such period may be of use also with modern challenges to electoral freedom.

249 It is doubtful that a concrete contribution to the victory of Donald Trump has come from the contribute of the data analysis of Cambridge Analytica. Firstly it is proved that similar methods were used also by the democrats and since Barack Obama victory of 2012 in which social network were massively used to carry on the campaign. Secondly the same tools have been used also to support Hilary Clinton's campaign which also made broad use of data analysis with political purposes. See in this respect R. J. GONZALES, cit., p. 11 and other authors mentioned in the paper such as E. HERSH, *Hacking the electorate*, Cambridge, 2015.

250 Even though the draft is not yet available several sources reported the news in the first weeks of August 2018 see e.g. *EU targets European political parties that misuse voters' data*, in *Financial Times*, 26th of August 2018 and *L'Ue vuole evitare un'altra Cambridge Analytica: multe ai partiti che usano i dati per la propria campagna*, in *La Repubblica*, 27th August 2018.

that use data harvested by virtue of illegal methods or privacy breaches and other circumstances similar to the Facebook-Cambridge Analytica scandal to carry on their campaign.

Moreover the regulation might include provisions focused on preventing political micro-targeting on social networks i.e. the practice of sending targeted and political messaging to users without their consent.

The Commission is also working on a set of recommendation to Member States in order to ensure the promotion of the highest level of transparency in political propaganda also under national legislations.

Such measures represent a new interesting type of approach to the matter since they are based on the *ratio* of keeping political parties liable for the use and the abuse of personal data with respect to electoral propaganda. Moreover the risk to pay the fine[251] may conduct the parties to avoid hiring certain data analysts in case of doubts on the transparency of the methods used by the latter to harvest and process data.

Finally a possible area of intervention could be the provision of legal mechanisms aimed at reducing the impact of fake news and the use of fake profiles to broadcast targeted political contents, forcing social networks and web corporations to promote a more effective control on online contents[252].

SIMONE PITTO

251 The amount of the fine, according to available sources, might be in the range of 5 per cent of the annual budget of a political party.

252 In such perspective many social media like Twitter have recently increased their efforts in identifying and removing fake profiles especially when they are used to broadcast political and targeted messages and terrorist propaganda and violence. It seems then that the Cambridge Analytica case has triggered a change of approach of social media like Twitter to political propaganda. See *Twitter, sospesi altri 486 account "manipolatori"*, in *La Repubblica*, 28th August 2018.

Panel II - Big Data and State Jurisdiction (the un-territoriality of data): how centrality of territoriality is challenged by the present-day dynamics governing the search and seizure of digitized information

II.1

The interface between the jurisdictional rules of Reg. (EU) No 2016/679 and those of Reg. (EU) No 1215/2012

SUMMARY: 1. Introduction. – 2. The interface between the jurisdictional rules of the GDPR and those of the B1R: Recital (147) GDPR and 67 B1R. – 3. Jurisdiction and coordination of multiple proceedings in the GDPR: Arts 79(2) and 81. – 4. The interface with Arts 4(1), 7, 18, 25, 26, 29 and 30 B1R. – 5. The interface in collective redress and mass harm situations. – 6. Conclusions.

1. In addition to administrative ones, Reg. (EU) No 2016/679 (hereafter "GDPR")[253] provides for private enforcement remedies that are purported to protect the fundamental right to data protection. In particular, where his rights are impaired by an infringement of the GDPR, the data subject entertains the right to an effective judicial remedy and to receive compensation, respectively under Arts 79(1) and 82(1) of the regulation.

Effective judicial remedies referred to in Art 79(1) GDPR are those provided for in the laws of each Member State (hereafter "MS"), and, in essence, injunctions[254] directed against a controller or processor (hereafter jointly referred to as "controller"). Furthermore, Art 82(1) GDPR grants the data subject the right to receive compensation for material and non-material damage resulting from the infringement of the regulation[255].

Considering that single infringements of the GDPR may affect a large number of data subjects simultaneously, Art 80(1) of the regulation provides that, where permitted by the laws of the MS courts seised, the rights granted by Art 79(1) and 82(1) of the same regulation may be exercised by the data subject through a «non-for-profit body, organisation or association».

Moreover, assuming that infringements of the right to data protection may have cross-border implications, the GDPR implements specific jurisdictional rules. Where disputes arising from infringements of the GDPR are characterized by an international element, Art 79(2) of the regulation determines the courts of which MSs may grant the remedies provided for in Art 79(1) and 82(1)[256] of the same regulation. Art 79(2) GDPR clearly favors the data subject[257], by allowing him to sue either in the courts of the MS where he habitually resides, or where the controller has an

253 Regulation (EU) No 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), OJ L 119/1, 4.5.2016, p. 1 ff (http://data.europa.eu/eli/reg/2016/679/oj).

254 See P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. DE FRANCESCHI (edited by), *European Contract Law and the Digital Single Market*, Cambridge-Antwerp-Portland, 2016, p. 97; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, in *RDIPP*, 2016, p. 667-668.

255 Recitals (75) and (85) GDPR provide examples of damage that may result from the infringements of the regulation.

256 See Art 82(6) GDPR.

257 On the protective policy underlying Art 79(2) GDPR, see L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, in *Stockholm Faculty of Law Research Paper Series*, 2018, p. 2 ff. Available at SSRN: https://ssrn.com/abstract=3159854 (accessed 15.8.2018); P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 97-98.

establishment[258].[259] Furthermore, Art 81 GDPR governs the coordination of proceedings concerning the same infringement of the regulation and instituted in the courts of different MSs.

However, the specific jurisdictional rules of the GDPR are not the only rules on the conflict of jurisdiction that may apply to disputes between data subjects and controllers. In particular, provided that such disputes are, in principle, civil and commercial in nature, where characterized by an international element, the general jurisdictional rules of Reg. (EU) No 1215/2012 (hereafter "the B1R")[260] may purport to be applicable to proceedings instituted under Art 79(1) and 82(1) GDPR[261].

2. The GDPR deals with the issue of the interface between its specific jurisdictional rules and the general ones of the B1R. Recital (147) GDPR stipulates that, general rules on jurisdiction of the B1R must not prejudice the application of the specific ones of the GDPR, «in particular as regards proceedings seeking a judicial remedy including compensation».

However, the recital is not reflected in any provision of the regulation, and, as such, it has an uncertain legal force[262]. Attention should thus be drawn on a provision of the B1R: Art 67, which actually inspired the wording of Recital (147) GDPR. «Shall not prejudice» are, in fact, the keywords in Recital (147) and Art 67 B1R. Akin to Recital (147) GDPR, Art 67 B1R provides that

258 This, by the way, gives the data subject the chance of suing the Third State controller in a MS, in all cases, even where the latter lacks an establishment in a MS. Cf. M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *IDPL*, 2015, p. 265.

259 For sake of completeness, Art 79(2) GDPR allows the data subject to sue in the courts of the MS where he habitually resides, unless the controller is a public authority of a MS in the exercise of its public powers. Certain scholars posit that, under Art 79(2) GDPR, the data subject should be allowed to sue the public authority in the courts of the MS where the latter has an establishment. However, the wording of the provision is not conclusive and the one employed in Recital (145) GDPR rather suggests that proceedings against a public authority acting in the exercise of its public powers fall outside the scope of the provision. Cf. M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, p. 272-273.

260 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), OJ L 351/1, 20.12.2012, p. 1 ff (http://data.europa.eu/eli/reg/2012/1215/oj).

261 The civil and commercial nature of disputes and the existence of an international element are in fact the two elements that define the scope *ratione materiae* of the B1R. In principle, following the findings of the CJEU in the *Eurocontrol* case, the first element is traced where the controller is a private party or a public authority acting in a private capacity, whereas it is excluded where the latter is acting in the exercise of its public powers. See C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669 and footnote 51; M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, p. 261-262, 272-273; and CJEU, 14.10.1976, C-29/76, *LTU Lufttransportunternehmen GmbH & Co. KG v Eurocontrol*, ECLI:EU:C:1976:137 (http://curia.europa.eu/juris/showPdf.jsf;jsessionid=77A4E0AAF7FC923395E75488EAF2BAF4?text=&docid=89285&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1160263).

262 See CJEU, 2.4.2009, C-134/08, *Hauptzollamt Bremen v J. E. Tyson Parketthandel GmbH hanse j.*, ECLI:EU:C:2009:229, point 16 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=73634&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1160390).

the latter regulation must «not prejudice the application of provisions governing jurisdiction[263] (…) in specific matters which are contained in instruments of the Union (…)»[264].

What follows from Art 67 B1R is that specific jurisdictional rules such as those of the GDPR, do not supersede the general rules of the former regulation, but rather prevail[265] «to the extent of any inconsistency» with the latter regulation[266]. In other words, the specific rules of the GDPR are not to be understood as *lex specialis* vis-à-vis the general ones of the B1R, but rather as a «*lex formidabilis*»[267]!

Hence, the rules on jurisdiction of the B1R must be disregarded whenever their application may «contradict (…) or affect the integrity and consistency of the special regime provided [in the GDPR]»[268], whereas in all other cases, the former rules may continue to be applicable[269]. This means that the rules of the B1R may still be applicable, unless their application hampers the jurisdictional favor granted to the data subject, by reducing the number of MSs where he may sue the controller under Art 79(2) GDPR[270], or by providing the latter with a greater number of MS courts where it may sue the former.

3. Art 79(2) GDPR governs jurisdiction over actions brought by data subjects – and, apparently, by NGOs too (§ 5) –, but does not cover actions brought by controllers, which instead may fall within the purview of the general rules of the B1R[271].

This said, the MS of habitual residence referred to in Art 79(2) GDPR is likely to be that where the infringement of the regulation affects the data subject, and, namely, where damage is

263 Unlike Recital (147) GDPR, mentioning «rules on jurisdiction», Art 67 B1R makes broader reference to «provisions governing jurisdiction», which thus covers both the special rule on jurisdiction (Art 79(2)) and that on coordination of proceedings (Art 81) of the GDPR.

264 Few pieces of EU legislation on specific matters contain jurisdictional rules. See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 31-32; A. DICKINSON, E. LEIN (eds.), *The Brussels I regulation recast*, Oxford, 2015, p. 564, footnote 4.

265 See A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo nel tempo (della "ateritorialità") di internet*, in *Europa e diritto privato*, 2017, p. 1197.

266 See A. DICKINSON, E. LEIN (eds.), *The Brussels I regulation recast*, p. 564.

267 G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, in *L'Observateur de Bruxelles*, July 2018, p. 29. Cf. L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 32 ff.

268 P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 104.

269 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, in *Cuadernos de Derecho Transacional*, 2017, p. 451; I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, in *Masaryk University Journal of Law and Technology*, 2017, p. 22 and footnote 59; P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 104; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669.

270 See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 33-34; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669.

271 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 451.

caused[272]. Though being used as a connecting factor also in other European private international law instruments, the notion of habitual residence within the meaning of Art 79(2) GDPR is far from being undisputed[273] and yet less controversial than that of establishment mentioned in the first period of the same provision.

As concerns the notion of establishment, it is submitted that, following the first period of Art 79(2) GDPR, the data subject may elect to sue in the MS where the controller has an establishment[274] and not only in that where the latter has its main establishment[275]. This gives the data subject a wider choice, since the notion of establishment in Recital (22) GDPR is broader than that of main establishment in Art 4(16) of the regulation[276].

272 See ID., p. 455.

273 Cf. G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, p. 29-30; L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 28-29; P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 101 ff.

274 Provided that the provision only refers to cases where the controller has an establishment in a MS, it should not apply where the controller has none. However, Kohler posits that the provision may vest jurisdiction in the courts of the MS of the representative appointed by a controller lacking establishments in a MS, in accordance with Art 27 GDPR. Actually, this opinion is backed by the last period of Recital (80) GDPR, which stipulates that enforcement proceedings should also be available against representatives. However, the recital is not reflected in any provision of the GDPR, including Art 79(2) thereof. Furthermore, in the *Weltimmo* case, the CJEU found that a processor had an establishment in a MS, by taking into account a number of facts, among which, the appointment of a representative with an address in that MS. It appears that, in principle, the mere appointment of a representative in a MS should not be sufficient to consider a controller as having an establishment in the same MS. Therefore, the preferred reading of the first period of Art 79(2) GDPR, is that the provision does not vest jurisdiction in the courts of the MS where a representative is based, unless it may qualify as an establishment within the meaning of the regulation. See C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 668; CJEU, 1.10.2015, C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639, points 32 ff (http://curia.europa.eu/juris/document/document.jsf?docid=168944&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=3527546).

275 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 453, echoing P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 99-100. But see L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 27-28, 34, according to which establishment referred in Art. 79(2) GDPR is actually to be understood as main establishment.

276 The recital reflects the «flexible definition» of establishment in Recital (19) Directive 95/46/EC, endorsed by the CJEU in the *Google Spain*, *Weltimmo* and *Wirtschaftsakademie* cases. See, respectively, CJEU, 14.5.2014, C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, point 49 (http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en); *Weltimmo*, points 32 ff; 5.6.2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, point 55 (curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3527736).

Generic reference to an establishment also implies that, though likely[277], the relevant establishment is not necessarily that where the infringement of the GDPR took place[278]. On the contrary, that is to say, if the data subject were required to fulfil the cumbersome task of proving that the infringement of the GDPR took place in the establishment located in the MS of the seised courts, the aim pursued by the regulation of granting the data subject with more favorable rules on jurisdiction could be undermined[279]. This is why, following a first reading, the establishment mentioned in Art 79(2) GDPR may lack any connection with the infringement of the regulation, even if this would admittedly encourage forum shopping by data subjects[280].

But a second and different reading should be preferred, one that better reflects the principles enshrined in the case law of the Court of Justice (hereafter "CJEU") on EU data protection legislation[281]. Following such case law, establishment is not just that where the unlawful handling of personal data took place, but also that in the context of whose activities such handling was carried out[282]. The latter being the case where such activities are «inextricably linked» with the unlawful handling[283]. If these findings were applied to the first period of Art 79(2) GDPR, then the provision could vest jurisdiction in the courts of the MS of the establishment where the infringement of the regulation took place, and where activities carried out were inextricably linked with the same infringement. Where followed, this reading could lower the risk of forum shopping and yet favor the data subject sufficiently[284].

The second reading should thus be preferred in that it better reflects the case law of the CJEU, whereas the first reading, a part from encouraging forum shopping, could lead to the application of Art 79(2) GDPR also in cases lacking an international element[285].

277 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 451; D. COOPER, C. KUNER, *Data Protection Law and International Dispute Resolution*, in *RCADI*, CCCLXXXII, 2017, p. 121.

278 See G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, p. 29; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 453.

279 See P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 100.

280 See ID., p. 101.

281 Namely, on Directive 95/46/EC and, in particular, on Art 4(1)(a) thereof.

282 See Art 3(1) and the first period of Recital (22) GDPR. See also the findings of the CJEU on Art 4(1)(a) Directive 95/46/EC in *Google Spain*, point 52, and *Wirtschaftsakademie Schleswig-Holstetin*, point 57.

283 See CJEU, *Google Spain*, points 51 ff; *Wirtschaftsakademie Schleswig-Holstein*, point 60.

284 However, alike the first, the second reading does not secure a strong connection between the seised court and the infringement of the GDPR in all cases. This is the consequence of taking the flexible notion of establishment, which is linked to a wider issue: the far reaching scope of European data protection legislation. Cf. I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 26 ff.

285 The international element that triggers the application of Art 79(2) GDPR consists in the difference between the MS where the data subject habitually resides and that where the establishment of the controller is located. The first reading examined above appears to imply that the existence of an establishment in a foreign MS may be sufficient to trigger the application of Art 79(2) GDRP. If so, the provision could be applicable in purely domestic cases, that is to say, where the data subject, the controller, the infringement and the damage caused are located in the same MS, insofar as the controller has an establishment in a different MS. Instead, following the second and preferred reading also examined

Drawing on Art 81 GDPR, the provision addresses the issue of multiple proceedings concerning «the same subject matter as regards processing by the same controller». Pursuant to Art 81(1) and (2) GDPR, where such proceedings are pending before the courts of different MSs, the MS court second seised may elect to suspend proceedings instituted before it, but only after having taken contact with the MS court first seised, to confirm the existence of proceedings concerning the processing by the same controller. Art 81(3) GDPR further provides that, where proceedings are pending at first instance before the MS court second seized, the latter may also, on application of one of the parties, decline jurisdiction if the MS court first seised has jurisdiction over the actions in question and its law permits consolidation thereof[286].

Recital (144) GDPR might suggest that Art 81 of the regulation only refers to proceedings instituted under Art 78 of the same regulation, that is to say against a decision by a supervisory authority[287].[288] However, the recital may not lead to a narrower reading of Art 81 GDPR and the broad wording of the provision suggests that it should also be applicable to multiple proceedings instituted under Art 79(2) of the regulation[289].

If this is correct, then a following question arises: whether the provision applies where multiple proceedings are instituted by data subjects only, or also where such proceedings are pending in parallel with those instituted by a controller, under different heads of jurisdiction, say Art 7(2) B1R (§ 4).

Though the wording of Art 81 GDPR appears to be broad enough to cover also the latter case, it has been held that, where multiple proceedings are instituted respectively by data subjects and controllers, their coordination should be governed by the general rules of the B1R and not those of the GDPR[290].

Unlike Art 81 GDPR, general rules of the B1R on related proceedings and *lis pendens* are based on the principle of temporal priority: the MS courts second seised must stay proceedings. As discussed below (§ 5), the principle enshrined in these general rules is inadequate in mass harm situations, such as those that may arise from infringements of the GDPR.

above, the international element may exist only if the MS where the data subject habitually resides is different from that of the establishment where the infringement of the GDPR took place, or where activities inextricably linked to the same infringement were carried out. There appears to be also another element that should be deemed international and thus trigger the application of Art 79(2) GDPR: damage resulting from the infringement of the regulation caused in a MS other than that where the data subject habitually resides.

286 This provision was clearly inspired from Art 30(2) B1R.

287 P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 106.

288 Actually, this reading may be upheld by referring to Art 76(3) and (4) of the proposed text of the GDPR. See Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection), COM(2012) 11 final, (http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf).

289 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 458 and footnote 29.

290 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 458 ff.

These are the reasons why the preferred reading of Art 81 GDPR is that the provision may apply in cases of multiple proceedings concerning the processing by the same controller, irrespective of the party that has instituted them.

4. Indeed, domestic courts, and, ultimately, the CJEU will have the last say as to which jurisdictional rules of the B1R will survive the GDPR[291]. In the meantime, scholars have faced the issue with reference to, in particular, Arts 4(1), 7, 18, 25, 26, 29 and 30 B1R, which respectively provide for the general head of jurisdiction, special heads of jurisdiction, the head of jurisdiction over consumer contracts, prorogation of jurisdiction, related proceedings and *lis pendens*.

Before examining each of the provisions mentioned above and the interface with the GDPR, it must be recalled that Art 79(2) of the regulation does not govern jurisdiction over actions brought by controllers, which instead may fall within the purview of the B1R.

Having this recalled, under Art 4(1) B1R, a person domiciled in a MS may be sued in the courts of that MS. This provision is not exactly the same as the one in the first period of Art 79(2) GDPR, since the notion of domicile is narrower than that of establishment within the meaning of the latter provision. In particular, when it comes to companies, following Art 63 B1R, domicile is the place of the MS where the company (or other legal person or association) has its statutory seat, central administration or principal place of business. As a consequence, where the place of domicile is not the establishment within the meaning of the first period of Art 79(2) GDPR, the data subject should be allowed to sue the controller also in the courts of the MS where the controller has its domicile under Arts 4(1) and 63 B1R[292].

Moving to special heads of jurisdiction of the B1R, these apply in addition to the general head of jurisdiction and thus, under the latter regulation, a claimant may elect whether to sue a defendant domiciled in a MS either in the courts mentioned in Art 4(1), or, alternatively, in those mentioned in Art 7 of the same regulation[293].

Art 7(1) B1R provides that, in matters relating to contract, courts having jurisdiction are those of the MS where the place of performance of the obligation in question is located[294]. It is submitted that, where the provisions of the GDPR are embedded in a contract between a data subject and a controller, and disputes arise from the infringement of the same provisions, the latter should also be allowed to sue in the courts of the MS mentioned in Art 7(1) B1R[295], which – though unlikely – may be different from those mentioned in Art 79(2) GDPR.

291 See I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 22.

292 See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 13; I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 22.

293 See Art 5(1) B1R.

294 See Art 7(1)(a) B1R.

295 See L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 13-14; C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669-670; M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 266.

Instead, where disputes concern contracts entered into by weaker parties[296], protective heads of jurisdiction apply[297]. These heads of jurisdiction take precedence over the other rules of the B1R[298] and purport to favor weaker parties on a jurisdictional level. Art 18 B1R deals with jurisdiction over consumers contracts. Akin to Art 79(2) GDPR, Art 18(1) B1R provides that a consumer may sue the professional either in the courts of the MS where he is domiciled or where the latter is based. Hence, where a contract embedding the provisions of the GDPR exists and the data subject is a consumer, the latter should be able to rely on Art 18 B1R[299], especially if his domicile is different from that where he habitually resides within the meaning of Art 79(2) GDPR.

Art 18 B1R also provides that the professional may sue the consumer only in the MS where the latter is domiciled[300]. Though clearly inspired by the protective rules on jurisdiction of the B1R, including Art 18 thereof, surprisingly, neither Art 79 GDPR, nor any other provision of the latter regulation, governs jurisdiction over actions brought by the controller against the data subject and thus, as repeatedly mentioned above, jurisdiction over such actions may be governed by the general rules of the B1R.

Drawing back to special heads of jurisdiction, under Art 7(2) B1R, in matters relating to tort jurisdiction lies with the court of the MS where the harmful event occurred or may occur. This is the provision of the B1R that has raised major debate among scholar as to the interface of the latter regulation and the GDPR.

Following the sc. ubiquity approach taken by the ECJ, Art 7(2) B1R vests jurisdiction both in the courts of the MS where damage is caused and in those of the MS where the event giving rise to it takes place[301].

In the specific case of claims for compensation of damages arising from the infringement of personality rights by means of content placed online on an internet website[302], the CJEU held that

296 During the recasting of Reg. (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, by its letter of 20 September 2011, the European Data Protection Supervisor urged the Commission to consider whether «jurisdictional rules [should] protect the weaker party also in data protection litigation». The proposal was dropped and, ultimately, only consumers, insured (policyholders and beneficiaries) and individual employees qualify as weaker parties under the B1R. See the letter of the 20th of September 2011, by the European Data Protection Authority, addressed to the Commission and bearing the following record number: GB/HH/et/D(2011)1571 C 2011-0106 (https://edps.europa.eu/sites/edp/files/publication/11-09-20_letter_reding_en.pdf).

297 See Sections 3, 4 and 5 B1R, which respectively apply in cases of insurance, consumer and individual employment contracts.

298 Except exclusive heads of jurisdiction in Art 23 B1R.

299 See M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 276-278. See also L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 14 ff.

300 See Art 18(2) B1R.

301 See CJEU, 30.11.1976, C-21/76, *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA.*, ECLI:EU:C:1976:166 (http://curia.europa.eu/juris/showPdf.jsf?text=&docid=89372&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3528393).

302 See, for further readings, M. A. LUPOI, *Attività online e criteri di collegamento giurisdizionale*, in *RTDPC*, 2018, p. 509 ff; Opinion of Advocate General Bobek, delivered on 13.7.2018, in C-194/16, *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB,* ECLI:EU:C:2017:554 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=195583&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3528548); B. HESS, *The Protection of Privacy in the Case Law of the CJEU*, in B. HESS, C. M. MARIOTTINI (eds.), *Protecting Privacy in Private*

courts having jurisdiction under Art 7(2) B1R are those of the MS where the injured party has his center of interests – which, though unlikely, may be different from his habitual residence – or those where the publisher is established, or, alternatively, those where the content placed online is or has been accessible[303]. Following such case law, in the first two cases, the courts have jurisdiction over damage to the injured party, wherever it was caused, whereas, in the third case, the courts of the MS have jurisdiction only over damage caused in that State[304].

Provided that, potentially, content placed online may be accessed in all 28 MSs, the courts of all such MSs could take jurisdiction, though only in relation to damage caused in their respective territory[305]. This solution leads to a fragmentation of jurisdiction amongst the courts of the MSs and is why the approach taken by the CJEU is known as the "mosaic" approach.

It is doubt whether the "mosaic" approach should extend to Art 79(2) GDPR[306]; the preferred reading is it should not[307]. In cases of claims for compensation of damages arising from the infringement of the right to data protection on the internet, the courts of the MS seised under Art 79(2) should be allowed to assess the entire damage suffered by the data subject, even where such courts are not those of the MS where the latter has his center of interests or where the controller is established[308]. If otherwise, the aim pursued by the GDPR of granting data subjects «full and effective compensation for the damage they have suffered»[309] could be undermined.

Furthermore, scholars disagree as to whether Art 79(2) GDPR may apply in parallel with Art 7(2) B1R, even if the latter provision admittedly increases the number of MS courts the data subject may rely on. Those who rule out the possibility stress that, if both provisions were applicable, in case of infringements of the right to data protection on the internet, data subjects would be granted

International and Procedural Law and Data Protection, Baden-Baden, 2015, p. 89 ff.

303 See CJEU, 25.10.2011, C-509/09 and C-161/10, *eDate Advertising GmbH and Others v X and Société MGN LIMITED*, ECLI:EU:C:2011:685 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3528601) and, most recently, 17.10.2018, C-194/16, *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB*, ECLI:EU:C:2017:766 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=195583&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3528684).

304 See CJEU, *eDate Advertising*, points 42 ff, citing CJEU, 7.3.2005, C-68/93, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA.*, ECLI:EU:C:1995:61 (http://curia.europa.eu/juris/showPdf.jsf?text=&docid=98911&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3528759), on a case of defamation through the press, where the court took, for the first time, the "mosaic" approach.

305 See Opinion of AG Bobek, in *Bolagsupplysningen*, points 77 and 80.

306 See G. VAN CLASTER, *Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée*, p. 29.

307 Cf. L. LUNDSTEDT, *International jurisdiction over cross-border private enforcement actions under the GDPR*, p. 29; M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 271.

308 In the *eDate Advertising* the notion of establishment is that taken in Directive 2000/31/EC, which appears to be slightly narrower than that of the GDPR. See CJEU, *eDate Advertising*, points 53 ff; Recital (19) 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"), OJ L 178, 17.7.2000, p. 1 ff (http://data.europa.eu/eli/dir/2000/31/oj).

309 Recital (146) GDPR.

an «overextended jurisdictional privilege»[310] and this «would harm the clarity and unity of the special regime laid down in Art 79(2) GDPR»[311].

Even if these assumptions were correct, there appears to be a reason why the concurrent application of Art 7(2) B1R and 79(2) GDPR should be endorsed.

Art 7(2) B1R governs jurisdiction also over actions brought by alleged tortfeasors for negative declarations seeking to establish the absence of their liability in tort[312]. Now, bearing in mind that jurisdiction over actions brought by controllers seeking a declaration of non-liability under the GDPR may be, in principle, governed by Art 7(2) B1R[313], if the latter provision were not applicable in parallel with Art 79(2) GDPR, then controllers could sue in a greater number of MSs than those where the data subject could. This imbalance would be even greater where the data subject were claiming together with data subjects from different MSs, through an Art 80(1) GDPR NGO, in which case, the only courts available would be those of the MS where the controller has an establishment (§ 5). All this appears to be inconsistent with the protective policy underlying the GDPR and is why a concurrent application of Art 79(2) thereof and Art 7(2) B1R should be endorsed.

Coming to prorogation of jurisdiction by consent, under Art 25 B1R, parties may agree that «the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise between them in connection with a particular legal relationship». A similar agreement on jurisdiction may be either exclusive or non-exclusive; it is exclusive where the parties have not agreed otherwise. Where exclusive, the agreement confers jurisdiction on the selected MS court and derogates jurisdiction of any other court, whereas a non-exclusive one only bestows authority upon the selected courts. This means that, where a non-exclusive jurisdiction agreement applies, a part from the selected MS courts, other courts may take jurisdiction over the prorogued disputes, insofar as they are provided with such under different rules of the B1R, say, for instance, Arts 4(1) or 7 thereof.

But a jurisdiction agreement may also be asymmetric. An asymmetric jurisdiction agreement is one which provides one of the parties with a greater number of courts to resort to. A particular kind of asymmetric agreements are sc. one-sided jurisdiction agreements, whereby one party may sue only in the courts of one State and the other may sue in the courts of that and other States. In other words, such a kind of jurisdiction agreements are exclusive for one party and non-exclusive for the other.

Similar agreements are the only that, according to the B1R, weaker parties, amongst which consumers, may enter into[314]. In fact, following Art 19 B1R, in case disputes have arisen between a consumer and a professional, the litigants may enter into a jurisdiction agreement according to

310 I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 23.

311 P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 105.

312 See CJEU, 25.10.2012, C-133/11, *Folien Fischer AG and Fofitec AG v Ritrama SpA*, ECLI:EU:C:2012:664 (curia.europa.eu/juris/document/document.jsf?text=&docid=128908&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3529058).

313 But see P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 92 and 105.

314 See Arts 15, 19 and 23 B1R.

which the consumer may sue in more MS courts than those made available in Art 18(1) B1R, whilst leaving the professional with no other choice than suing in the courts where the same consumer is domiciled.

Under the GDPR, jurisdiction agreements should be permitted, as far as they increase the number of MS courts where the data subject may sue the controller[315], whilst reducing or leaving unaffected the number of MS courts made available to the controller. Hence, a one-sided jurisdiction agreement favoring the data subject should be permitted, whereas an exclusive or a non-exclusive jurisdiction agreement should not[316].

This said, prorogation of jurisdiction may also take place tacitly. According to Art 26 B1R, tacit prorogation of jurisdiction occurs when a party enters into an appearance before the court of a MS without challenging jurisdiction, thereby vesting the seised court with such. Art 26(2) B1R provides that, where the defendant is a weaker party, such as a consumer, the seised courts must inform the latter that he may contest jurisdiction and the consequences of entering or not an appearance.

Also the latter provision of the B1R should be applicable in parallel with the jurisdictional rules of the GDPR, unless the data subject is the defendant[317]. In the latter case, where the data subject is the defendant, Art 26 B1R should not be applicable[318], or, perhaps, it could be, insofar as the latter be granted the same protection weaker parties enjoy under the second paragraph of the provision.

Drawing on the rules on the coordination of proceedings provided for in the B1R, Art 29 thereof deals with the case of «proceedings involving the same cause of action and between the same parties brought before the courts of different MSs», whilst following Art 30 of the regulation deals with «related actions (…) pending in the courts of different MSs». In essence, these rules aim at preventing conflicting decisions and, in both cases, this risk is addressed by providing that the MS courts second seised must stay proceedings and, where applicable, decline jurisdiction in favor of the MS courts first seised[319]. Unless an exclusive jurisdiction agreement applies[320], the courts second seised have no discretion. On the contrary, Art 81 GDPR leaves the MS courts second seised free to elect whether to stay proceedings[321].

315 See I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 23-24; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 452; P. FRANZINA, *Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, p. 107-108.

316 Cf. C. KOHLER, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, p. 669.

317 See F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I*-bis*"*, p. 452.

318 See I. REVOLIDIS, *Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?*, p. 24-25.

319 See, respectively, Arts 29(1) and 30(2) B1R.

320 See Art 31(2) B1R.

321 See above § 2.

Where proceedings concern the processing by the same controller, it appears that the latter provision should take precedence over Arts 29 and 30 B1R[322]. This, as mentioned above (§ 3), in the light of the broad wording of Art 81 GDPR and for the further reasons discussed below (§ 5).

5. Infringements of data protection legislation often affect a large number of data subjects based in different States and, in mass harm situations, injured parties are keen to seek redress collectively, rather than separately.

I t is likely that the assumptions above were the basis for Art 80(1) GDPR, according to which the rights granted by Art 79(1) and 82(1) of the regulation may be exercised by data subjects collectively through a «non-for-profit body, organisation or association»[323], to the extent that the laws of the MS courts seised permit collective actions[324]. Actually, despite Recommendation 2013/396/EU encouraging MSs to introduce injunctive and compensatory collective redress mechanisms for the implementation of rights granted under EU law[325], not all MSs have[326] and only in a small number of them such mechanisms appear to be «relatively well-functioning»[327].[328]

This said, the GDPR does not provide for a specific rule on jurisdiction applicable to collective claims[329]. Nonetheless, Art 79(2) GDPR should also be deemed applicable where the claimant is an NGO seeking an effective judicial remedy or compensation on the behalf of data subjects. In fact, though Art 79(1) GDPR speaks of the data subject's right to an effective judicial remedy, the second paragraph of the provision only mentions court proceedings instituted against a controller. The wording of Art 79(2) GDPR thus suggests that the scope *ratione personae* of the

322 Cfr. A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo nel tempo (della "aterittorialità") di internet*, 1199.

323 For sake of completeness, the second and last paragraph of Art 80 GDPR stipulates that MSs may provide that NGOs may exercise the right referred to in Art 79 – but not that referred to in Art 82(1) – autonomously.

324 Art 80(1) GDPR further provides that the NGO may represent the data subject, as far as it has been «properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of the data subjects' rights and freedoms with regard to the protection of their personal data».

325 Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU), in OJ L 201, 26.7.2013, p. 60 ff (http://data.europa.eu/eli/reco/2013/396/oj).

326 See Report from the Commission to the Parliament, the Council and the European Economic and Social Committee on the implementation of the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU), COM(2018) 40 final (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:40:FIN).

327 On the shortcomings of collective redress in the EU and the need for a uniform framework of law in the field of data protection, see L. JANČIŪTĖ, *Data protection and the construction of collective redress in Europe: exploring challenges and opportunities* (February 27, 2018). Available at: https://ssrn.com/abstract=3136040 (accessed 15.8.2018).

328 Most recently, on the 11th of April 2018, the European Parliament and the Council passed a proposal for a directive on representative actions for protection of the collective interests of consumers, which should cover «a variety of areas such as data protection». See Recital (6) Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM(2018) 184 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0184).

329 See M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International Data Privacy Law*, p. 273.

provision is determined by the defendant (a controller or processor) and regardless of who the claimant is[330]. Furthermore, Art 80(1) GDPR provides that the NGO may exercise the right to receive compensation on behalf of data subjects, whilst Art 82(6) of the regulation provides that proceedings for exercising such right shall be instituted in the MS courts referred to in Art 79(2) of the same regulation. Hence, the combined reading of Art 80(1) and 82(6) GDPR further suggests that Art 79(2) of the regulation might be applicable where the NGO is appointed by the data subjects to seek compensation on their behalf.[331]

If so, where data subjects have their habitual residence in the same MS, Art 79(2) GDPR should allow the NGO to sue either before the courts of that MS or those of the MS where the controller has an establishment, provided that – it must be recalled – the laws of such MSs permit collective actions. Instead, in the case where the data subjects have their habitual residence in different MSs, the NGO they have appointed should be allowed to sue on their behalf only in the courts of the MSs where the controller has an establishment, since the courts of the MS where only part of the data subjects have their habitual residence would be lacking jurisdiction with respect to the rest of them.

What follows from the above is also that, where data subjects acting collectively have their habitual residence in different MSs, Art 79(2) GDPR could provide the appointed NGO with just one forum, that of the MS where the controller has an establishment, as far as – once again – the laws of such MS permit collective actions.

If this is correct and if Art 79(2) GDPR were the only applicable head of jurisdiction in similar cases, a controller could prevent the risk of being the subject of a collective action brought by an NGO appointed by data subjects habitually residing in different MS, by placing its one and only establishment in a MS where collective claims are not permitted or difficult to be pursued.

But Art 79(2) GDPR should not be the only head of jurisdiction NGOs should be able to rely on. NGOs should also be allowed to sue in the courts of the MSs having jurisdiction under Art 4(1) and 7(2) B1R. In fact, though also heads of jurisdiction of the B1R are ill-suited for collective actions, the two provisions of the latter regulation allow several claimants to sue one or more defendants in the courts of the same MS simultaneously[332].

330 See also Recital (145) GDPR, which refers to the «plaintiff», rather than to the «data subject».

331 On the contrary, as underlined by Lein, the head of jurisdiction over consumer contracts in Art 19 B1R is «lost in cases in which an association or representative is acting for the consumers». In fact, the CJEU holds that the head of jurisdiction applies only where the consumer is, «in his personal capacity, the plaintiff or defendant», provided that, in accordance with the wording of Art 16 Reg. (EC) No 44/2001 (today, Art 19 B1R), the provision applies «only to an action brought by a consumer against the other party to the contract, which necessarily implies that a contract has been concluded by the consumer with the trader or professional concerned». Nonetheless, there are strong reasons why the rule on jurisdiction should be opened to class actions. See, respectively, E. LEIN, *Cross-Border Collective Redress and Jurisdiction under Brussels I: A Mismatch*, in D. FAIRGRIEVE, E. LEIN (eds.), *Extraterritoriality and Collective Redress*, Oxford, 2012, p. 135; CJEU, 25.1.2018, C-498/16, *Maximilian Schrems v Facebook Ireland Limited*, ECLI:EU:C:2018:37, points 44 and 45 and the case law cited therein (http://curia.europa.eu/juris/document/document.jsf?text=&docid=198764&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3530052); M. MORANI, *L'azione di classe in Europa, aspettando la Corte di giustizia europea sul caso Schrems vs. Facebook*, in *Int'l Lis*, 2016.

332 See A. STRADLER, *The Commission's Recommendation on Common Principles of Collective Redress and Private International Law,* in E. LEIN, D. FIRGRIEVE, M. OTERO CRESPO, V. SMITH (eds.), *Collective Redress in Europe – Why and How?*, London, 2015, p. 242 ff; E. LEIN, *Cross-Border Collective Redress and Jurisdiction under Brussels I: A*

The reason why NGOs should be allowed to bring collective claims also in the courts mentioned in Arts 4(1) and 7(2) B1R is that, on the contrary, the controller could resort to a greater number of MS courts, where to file an action seeking a declaration of non-liability under Art 7(2) B1R[333].

Conversely, it is submitted that rules on the coordination of jurisdiction set forth in the B1R based on the principle of temporal priority do not «provide adequate solutions» in mass harm situations, where «there is a high probability that [such situations] will be picked up by various representative associations or claimants in different Member States»[334].

In similar situations, where harm results from the same infringement of the GDPR, if the general rules of the B1R were applicable, the instituting of proceedings by a single data subject or NGO in the courts of a Member State could block the proceedings instituted by the other injured data subjects or Art 80(1) GDPR NGOs in the courts of a different MS. The data subjects or Art 80(1) GDPR NGOs would be tripping themselves… Furthermore, if such general rules were deemed applicable, controllers could be encouraged to practice "forum running": to sue first in the most favorable courts and block any following proceeding instituted by the data subjects or NGOs in a different MS.

Hence, in mass harm situations, a rule bestowing discretion upon the Member State courts second seised, such as that in Art 81 GDPR, appears to be consistent with the protective policy underlying the regulation, as well as a more appropriate rule in mass harm situations[335]. Besides, Art 81 GDPR, addresses the risk of conflicting decisions adequately, by placing on the MS court second seised the duty to take contacts with the MS court first seised.

This is the reasons why, a part from the far reaching wording employed in Art 81 GDPR, Arts 29 and 30 B1R should be no longer deemed applicable where multiple proceedings concern the processing by the same controller.

6. The parallel application of the heads of jurisdiction of the GDPR and those of the B1R might be a "forensic nightmare", but it should be endorsed to the largest extent possible.

Most of the issues examined above appear to be the result of a drafting shortcoming in Art 79(2) GDPR: unlike protective heads of jurisdiction of the B1R, the provision does not deal with jurisdiction over actions brought by the stronger party, the controller. As a consequence, provided that the controller may rely on the rules of the B1R, the data subject should be allowed to rely on the same rules too. If otherwise, especially in the case of actions in tort and those brought by NGOs, there is a risk that the data subjects may resort to a lower number of MS courts than those made available to the controller, and this would be inconsistent with the protective policy underlying the GDPR.

Mismatch, p. 132 ff.

333 This is true to the extent that it is submitted that the jurisdictional favor that reflects the protective policy underlying the GDPR also concerns NGOs.

334 A. STADLER, *Focus on Collective Redress: Cross-border Problems*. Available at https://www.collectiveredress.org/collective-border-problems (accessed 15.8.2018). See also ID, *The Commission's Recommendation*, p. 247-248.

335 But see A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo nel tempo (della "aterittorialità") di internet*, p. 1199.

Conversely, since they appear to be inadequate in mass harm situation, in cases where multiple proceedings concern the processing by the same controller, rules on the coordination of such proceedings provided for in the B1R should no longer be deemed applicable.

In conclusion, though criticized by most scholars, yet the jurisdictional rules of the GDPR represent an effort that must be praised, in that they are the first known uniform rules that govern jurisdiction over civil and commercial claims in matters relating to the right to data protection.

ENNIO PIOVESANI

II.2

Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?

SUMMARY: 1. The argument and background of the paper. – 2. An overview of the *U.S. v. Microsoft* litigation and the U.S. Cloud Act. – 3. Possible motivations for a *comity-upon-request* rule and the "information problem". – 4. Assumptions and observations supporting the "information problem" view. – 5. Clashing state interests: Securitization of private data flows and the facilitation of global market access. – 6. Data location as a connecting factor. – 7. The proxy theory of connecting factors. – 8. Conclusion.

1. This paper focuses on a new framework provided by the U.S. "Clarifying Lawful Overseas Use of Data Act" (hereinafter "Cloud Act")[336] that is designed overcome jurisdictional conflicts with regards to law enforcement orders compelling service providers to disclose user data that is stored abroad on cloud computing based systems.

The Cloud Act was passed by the Congress in March 2018, bundled in a yearly budget act and passed without much discussion in the legislature. The Cloud Act seeks to circumvent the jurisdictional problem by authorizing disclosure warrants compelling service providers resident in the U.S. to disclose user information to U.S. authorities wherever the information is stored, but at the same time allowing the service provider to move to quash the compelling order ("warrant") in cases where the service provider finds it on its own initiative and discretion that the compliance with the order risks giving rise to a conflict of laws. The law sets guidelines for a "comity" assessment that the court will undertake upon a motion to quash duly made by the service provider. I argue that a motivation on the part of the U.S. government to create such a solution may be an interest in facilitating global market access of U.S. service providers without forfeiting more of its prescriptive authority than necessary. I further argue that this motivation should be studied as a universal central trend that is shaping the global regulation of data flows.

336 *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, H.R. 4943, enacted by *Consolidated Appropriations Act, 2018*, Pub. L. 115-141, 23 March 2018 (https://www.gpo.gov/fdsys/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm).

2. The Cloud Act became law just in time to render the *U.S.* v. *Microsoft* [337] (hereinafter "*Microsoft*") case before the U.S. Supreme Court moot, dodging (at least for a time) international repercussions that would result from a generally applicable Supreme Court judgment. That case concerned the refusal of Microsoft Corporation to disclose to the FBI user data that was stored in a data center located in Ireland upon the service of a disclosure warrant issued by a U.S. court, arguing that the warrant constituted an unlawful extraterritorial application of the Stored Communications Act (SCA) under which the disclosure warrant was provided for.[338] A generally applicable Supreme Court judgment would be problematic whichever party prevailed at the end, because it would either force the U.S. internet service providers to disclose user information wherever in the world that the information was stored, or it would foreclose the access of U.S. law enforcement to user data stored abroad in all cases, even when the crime and suspect was closely connected to the U.S.

The Cloud Act was drafted and passed following debates that focused on whether data location could be a feasible determinant of which state had prescriptive and enforcement jurisdiction over the compelled disclosure by law enforcement of user data with regard to cloud computing based services. Major U.S. service providers were apprehensive of the penalties they might face if they disclosed to U.S. law enforcement (upon a warrant from a U.S. court) data located in other countries that had strict rules on international personal data transfers. The EU General Data Protection Regulation (GDPR)[339] in particular proved to be very problematic due to the fact that (i) Europe was one of the major export markets of major U.S. cloud providers, (ii) a combination of court cases (such as *Google Spain*[340]) that strengthened the reach of the EU personal data protection rules to a broader range of service provider activity and the consolidation of the view in Europe that personal data protection rules should exclusively regulate law enforcement cooperation with third countries[341], and (iii) the GDPR prescribed very substantial penalties for violation of third country transfer rules.[342] American law enforcement worried that without the authority to compel disclosure of data located abroad, it would not be possible to collect evidence in many crimes that exclusively concerned the United States or U.S. persons, since Mutual Legal Assistance Treaties were not efficient in the timely collection of electronic evidence.[343] The government of the United Kingdom also had a prominent voice in these discussions, and they

337 *United States v. Microsoft Corporation,* 584 U.S. ___ (2018). (https://www.oyez.org/cases/2017/17-2).

338 18 U.S.C. § 2703, (https://www.law.cornell.edu/uscode/text/18/2703).

339 *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*, OJ L 119, 4.5.2016, p. 1–88, (http://data.europa.eu/eli/reg/2016/679/oj).

340 *Google Spain v AEPD and Mario Costeja González,* Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

341 The latter can be evidenced in the (ex) Article 29 Working Party's position related to the Council of Europe Budapest Cybercrime Convention. The WP29 strongly advocated against any interpretation of Articles 18 and 32 of that Convention that might undermine the application of the GDPR's data transfer regime to criminal law enforcement cooperation with third countries. See EUROPEAN COMMISSION ARTICLE 29 WORKING PARTY, *Data Protection and Privacy Aspects of Cross-Border Access to Electronic Evidence,* statement of 29 November 2017 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

342 See B. SMITH, *Written Testimony of Brad Smith President and Chief Legal Officer, Microsoft Corporation submitted the U.S. Senate Subcommittee on Crime and Terrorism,* 10 May 2017 (https://www.judiciary.senate.gov/download/05-24-17-smith-testimony).

advocated for either setting up a bilateral framework that allowed the two governments to directly request the disclosure of user data from service providers in cases where the crime was exclusively related to one of the states and their residents, wherever the data is located.[344] As to contributions from academia, two voices distinguished themselves. Jennifer Daskal, who was one of the main proponent of the Cloud Act in academia, argued that the nature of data increasingly created a discrepancy between the outcome that a data location based territorial rule is expected to yield in terms of a stratification between the several sovereign interests involved, and the real outcome created when that territorial rule is applied and enforced in practice.[345] Daskal argued that the solution necessarily required a multilateral approach at the international level. *Contra* Daskal, Andrew Woods turned to conflict of laws methodologies for the solution. According to his point of view, data does not offer a special difficulty, and the conflict of laws discipline has the necessary tools in its disposal to deal with the conflicting interests, largely on a case by case basis, and to create new guiding principles to equitably distribute prescriptive and enforcement powers to the sovereigns involved. Woods suggested that the abovementioned discrepancies between expected outcomes and real outcomes be overcome by courts employing some type of governmental interest analysis.[346] For American commentators, reference to a governmental/state interest analysis is informed by American common law that incorporates various choice-of-law methodologies developed as a result of the so-called American Conflicts Revolution.[347] In Europe, on the other hand, there is generally less doctrinal ground on which courts can explicitly analyze the conflicting interests on a case by case basis.

The Cloud Act creates two new statutory rights for service providers. 18 U.S.C. §2702(b)(9) stipulates that service providers may voluntarily disclose the contents of communications held in electronic storage, or carried or maintained by the provider to foreign governments upon request given that the foreign government is party to an executive agreement pursuant to §2523. §2702(c)(7) provides the same right in relation to customer records. Direct disclosures of user content data to foreign governments were explicitly forbidden under the previous version of the law. The second statutory right is the right to file a motion to quash or modify a warrant obtained from a U.S. court for disclosure of user data *only if* the disclosure would require the service provider to violate the law of a foreign government qualified by executive agreement *and* the subject of the warrant is not a U.S. person or U.S. resident (§2703(h)(2)). Upon this motion, the court will make a «comity

343 «the MLA process can lack the requisite efficiency for time-sensitive investigations and other emergencies, making it an impractical alternative to SCA warrants in many cases» B. WIEGMAN, *Statement of Brad Wiegman U.S. Deputy Ass't Att'y Gen. before the U.S. Senate Subcommittee on Crime and Terrorism*, 24 May 2017, p.6 (https://www.judiciary.senate.gov/download/05-24-17-wiegmann-testimony); «[MLATs] are widely regarded in the law enforcement community as a wholly ineffective alternative to obtaining evidence.» R. LITTLEHALE, *Written Statement by Richard Littlehale Special Agent in Charge Tennessee Bureau of Investigation submitted to the United States House of Representatives Committee on the Judiciary*, June 15, 2017, p. 2 (https://judiciary.house.gov/wp-content/uploads/2017/06/Littlehale-Testimony.pdf).

344 P. MCGUINNESS, *Written Testimony of Mr Paddy McGuinness United Kingdom Deputy National Security Adviser submitted the U.S. Senate Subcommittee on Crime and Terrorism*, 10 May 2017, (https://www.judiciary.senate.gov/download/05-24-17-mcguinness-testimony).

345 J. DASKAL, *The Un-Territoriality of Data,* in *YLJ*, 2005, p. 326.

346 A. K. WOODS, *Against Data Exceptionalism,* in *SLR*, 2016, p.729.

347 S. C. SYMEONIDES, *The American Choice-of-Law Revolution: Past, Present and Future,* Leiden, 2006.

analysis» by considering the specific factors provided under §2703(h)(3). This comity analysis that is done upon motion (which I call "*comity-upon-request*" in line with the argument of this paper) is explicitly distinguished in the text of law from the ordinary comity doctrine under American common law. Also, service providers may notify qualified foreign governments in cases where a disclosure of data process concerns data belonging to their nationals or residents, which would be illegal under the previous version of the law.

American critics of the new law have mostly focused on another set of provisions in the law that relax the SCA's previous categorical ban on the disclosure of user content data to foreign law enforcement by allowing U.S. service providers to disclose user content to criminal justice authorities of foreign governments that have signed an executive agreement with the U.S. government.[348] These critics fear that direct foreign government access to U.S. provider held user data could be used to circumvent U.S. rules regarding user privacy, since the executive agreement framework does not require foreign legal systems that will be authorized to have a probable cause standard for compelled search and seizure equivalent to the U.S. standard and the data acquired could end up being used in U.S. lawsuits, which is especially problematic if data regarding U.S. persons are also acquired in the process although the executive agreement framework requires foreign governments to adopt data minimization procedures to filter out and eliminate data that may be connected to U.S. persons.[349] These critics also point at the danger that the relaxation of the absolute disclosure ban may result in "bad states" accessing data of users.

3. The important privacy and evidence-standard implications of the Cloud Act notwithstanding, in this paper I want to focus instead on the *comity-upon-request* rule and its possible motivations and logic. I argue that the *comity-upon-request* rule might be motivated by an information problem that is the result of an effort to recalibrate and use conflict of laws methodology to facilitate corporate access to a global data storage and processing market. As data storage is a commodity in these markets, the fact that data location (which is an inalienable physical property of data storage) is imbued with jurisdictional claims by legal systems creates compliance-related costs but also costs related to legal uncertainty. A legal system, which in turn seeks to facilitate its domestic corporations access to a foreign data (storage) market can forfeit a part of its own prescriptive and enforcement authority in order to reduce the potential for conflict of laws that create such costs; but such a forfeiture has its own social and political costs as forfeiture of authority (which corresponds to deference to a foreign legal system) means a decrease in the state's

348 18 U.S.C. §2523, (http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2523&num=0&edition=prelim).

349 Electronic Frontier Foundation: C. FISCHER, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data,* 8 February 2018 (https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data); D. RUIZ, *Responsibility Deflected, the CLOUD Act Passes,* 22 March 2018, (https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes); K. RODRIGUEZ, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom,* 9 April 2018, (https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom); American Civil Liberties Union (ACLU): N. S. GULIANI, N. SHAH, *Proposed CLOUD Act Would Let Bad Foreign Governments Demand Data From US Companies Without Checks and Balances*, 19 March 2018, (https://www.aclu.org/blog/privacy-technology/consumer-privacy/proposed-cloud-act-would-let-bad-foreign-governments-demand); Electronic Privacy Information Center (EPIC): *The CLOUD A*ct (https://epic.org/privacy/cloud-act/).

capacity to realize public policy, e.g. prosecuting child pornography or drug sales as in the *Microsoft* case.

On the other hand, testimonial evidence suggests that although, theoretically, the risk of conflict of laws is high in scenarios where more than one legal system has a veritable jurisdictional claim on the activity in question, in practice, U.S. service providers have not met substantial opposition by other states when they were disclosing user data stored on their territories to U.S. law enforcement; that is until the U.S. service providers *themselves* started objecting to the practice.[350] If this was indeed the case in practice, then facilitating global market access via forfeiting prescriptive authority in anticipation of (theoretical) costs of conflict of laws might possibly be overcompensating this risk at a high social and political cost.

Herein lies what I call the information problem. Due to the lack of information as to the possibility of foreign legal systems claiming (or not claiming) jurisdiction where they have typically have not (or have), which partly results from the fact that the matter of international cooperation in law enforcement is typically managed in the bureaucratic level that is susceptible to capricious changes in practice, the legal system (both the legislative and the courts) cannot efficiently calculate the costs to corporations of conflicts of laws and thus balance *ex ante* these costs with the costs of forfeiture of authority. The *comity-upon-request* solution thus makes use of the corporation's own intelligence, know-how, and legal resources to assess scenarios when a U.S. court's warrant for worldwide disclosure of user data would be opposed by a foreign legal system, and require the U.S. to forfeit authority only in these scenarios but not in others where such a warrant could be fulfilled without opposition.

The information problem introduced above can be analyzed in finer detail to assess the merits of the proposed solutions and predict future uses of regimes similar to that in the Cloud Act. I propose a preliminary analysis of the information problem suggesting that legislators and government organs are faced with three types of information problems when deciding whether to assert prescriptive and enforcement jurisdiction in cases concerning data flows:

The three information problems

The general political information problem: Following the failure of activity location as a proxy, courts and the State cannot determine the extent of its interests affected in a given conflict. The corporate actor is "closer" to the conflict and its (economic and political) fallout.

The special political information problem: In the light of its role vis-à-vis the corporate actor, the State cannot determine with high certainty the outcome relative to the interests of the corporate actor, and application of proxy rules do not provide enough flexibility to the State to achieve results in line with the State's role vis-à-vis the corporate actor.

The judicial information problem: The courts do not have sufficient information to

350 See B. SMITH, *Written Testimony of Brad Smith President and Chief Legal Officer, Microsoft Corporation submitted the U.S. Senate Subcommittee on Crime and Terrorism*, cit.

ascertain the exact outcome relative to interests at stake preferred by the political branches. This is not a new problem, but is exacerbated by the dynamics of the modern economy, and increased rate of technological change that makes policy inherent in certain rules obsolete at a rate that the political branches cannot keep pace.

4. My interpretation of the motivations of the Cloud Act is based on two assumptions based on observations that will be discussed in this paper. The first assumption is that the facilitation of global market entry for corporate subjects is genuinely identified as a central interest of the state in the context of the application of conflict of laws methodology. The second assumption is that connecting factors such as data location can be thought of having intrinsic links with certain interests, to the effect that a shift in the perception of its interests would be a motivation for a state to abandon it for the sake of a connecting factor that is more instrumental to its newly perceived interests. I shall call this second assumption the proxy theory of connecting factors.

If these assumptions hold and my interpretation of the Cloud Act framework is workable, then this might yield insight helpful to predict future directions for the regulation of data flows and big data applications from a perspective different from substantive privacy law by placing the issue in a broader context of globalization and global governance. The use of conflict of laws methodology, including doctrines of comity, to facilitate corporations' participation in global denationalized markets by enabling corporations to release themselves from national jurisdictions is discussed in the literature and advocated by some commentators to be the correct path that the conflict of laws/private international law scholarship should take to remain relevant in the contemporary legal environment, where non-state private actors are competing with states for legitimacy in norm creation.[351]

The approach I am advocating will also help filling a gap in critical commentary of the ongoing trend of "privatization" of data flow regulation, such that directed at "the right to be forgotten" regime set after the ECJ decision in the *Google Spain* case. For instance, comments coming from the Electronic Frontier Foundation (EFF) regarding the Cloud Act and similar proposals in Europe appear to suggest that the "privatization" of the legal safeguards and assessment processes in both sides of the Atlantic have their basis in a lack of political will to uphold digital privacy rights. An innate inclination to surveil its citizenry that is frequently attributed to the nation state is a usual suspect in these critiques, however, in light of the structural and procedural distinction between criminal law instruments and national security instruments, and the hybrid character of these novel types of regulation, this explanation seems unsatisfactory. Thus, an explanation that accounts for the motivations for such policies of "privatization" and how they

351 R. WAI, *Transnational Liftoff and Juridical Touchdown: The Regulatory Function of Private International Law in an Era of Globalization,* in *CJTL*, 2002, p. 209; H. MUIR-WATT, *Private International Law Beyond the Schism,* in *TLT*, 2011, p. 347. I additionally argue that recent developments in the U.S. yields further evidence of the existence of a global market access facilitation motif also in the field of U.S. personal jurisdiction, whereby the exposure of large multinational companies to litigation in state courts are being significantly lowered as the U.S. Supreme Court adopts a stricter general/specific personal jurisdiction distinction akin to the Brussels (recast) regime in the EU, however made even more advantageous to multinationals due to specific additional doctrines of U.S. personal jurisdiction law**.**

are legitimized through joint appeals to both commercial necessities and security threats without relying too much on essentialist assumptions about the state could be useful.

5. The following factors can be identified as main governmental interests that could clash with each other, requiring a novel approach to jurisdictional rules that might make use of "privatizing" frameworks, such as comity-upon-request in the Cloud Act.

(1) Securitization of private data flows: The last decade has seen a proliferation of perceived online threats emanating from private persons or private groups. Social media and other web 2.0 applications have enabled certain types of private behavior that threatens public safety such as online radicalization and/or the spreading of disinformation regarding to all kinds of societal events. The perceived increase of such threats combined with the fact that the relevant medium of the threat is increasingly based on cloud computing technology, creates a motive for states that I call the "securitization" of private data flows. Securitization of cross-border communications is of course nothing new, it is arguably as old as the invention of writing systems, but at the very least it predates the popularization of cloud computing.[352] Instead, what I refer to by the securitization of data flows is a distinct phenomenon. I mean the perception of digital communications as a medium that is extremely conducive to hostile activities against the state and/or social order due to its enormous capacity to reach private citizens and the public domain. This perception guides the stance of the security apparatus of the state including criminal justice, national security, and military departments.[353]

The threat that securitization of private data flows envisions is typically derived from communications directed to persons located within the territory of the state, originating from persons, or groups, that may be located inside or outside of the territory of the state. From this perspective, the use of virtual networks, shell user accounts, automated bots, or other clandestine techniques render determinations of applicable law based on physical origin of the communication irrelevant to the state interest that is impacted by the communication, while the fortuitous connection between the communication and origin state offer poor justification for exclusively

352 Samuel Morland, an officer in the Royal Mail under Oliver Cromwell, on surveillance of private letters: «A skillful prince ought to make a watchtower of his general post office and there place such careful sentinels as that by their care and diligence he may have a constant view of all that passes. By the frequent inspection of letters a king soon know the temper of all his principle and active subjects.» T. SIMPSON, *Liberty and Surveillance: What Governments and Private Corporations Know About You?*, CIS Occasional Paper 162, 2018, p. 7, (https://www.cis.org.au/app/uploads/2018/01/op162.pdf).

353 Securitization of data flows happen on a wide continuum that extends from policing petty criminality to conducting counterterrorism and at the extreme, militarization of cyberspace. In June 2017, following a long period of efforts and discussions since 2004, the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security failed to finalize a document concerning how international law applies to States' use of ICTs, due to a lack of consensus on whether malicious use of ICTs could be considered as an "armed attack" as a matter of *jus ad bello*, and whether humanitarian law would apply to ICT-based operations of security forces. A. M. SUKUMAR, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, 4 July 2017, (lawfareblog.com, archived at https://perma.cc/5QZY-GUVD). Also see U.S. envoy to the GGE Michele G. Markoff's statement concerning the failure to reach a consensus: M. G. MARKOFF, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, 23 June 2017, (https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm).

determining prescriptive jurisdiction on the basis of location.[354] This puts the pressure on judicial systems to claim prescriptive and enforcement authority based on effects felt within their territories (inasmuch as territoriality remains as a proxy for a great majority of other state interests). This pressure may sometimes result in a government position that is unilateralist (some may say realist):

> «Congress did not enact a disclosure scheme that a U.S. provider could nullify by the expedient of shifting data to storage devices that it locates over the border. To allow that result would permit a private provider in the United States to thwart Section 2703's critical role in assisting law enforcement to combat terrorism and crime.» (Brief for the United States in *U.S.* v. *Microsoft*).[355]

> «the possibility of a future conflict between U.S. and foreign law does not change the best construction of an important domestic law enforcement and counterterrorism tool enacted more than 30 years ago.» (ibid.)[356]

> «it takes on average about 10 months to obtain communications from a U.S. Provider in response to an MLAT [Mutual Legal Assistance Treaty] request, and can take even longer. This is not timely enough to be useful to the U.K.'s law enforcement when they are trying to anticipate and head off terrorist and security threats or stop ongoing crimes such as drug trafficking and child abuse.» (Amicus Brief for the U.K in *U.S v. Microsoft*).[357]

The last testimony regarding the failure of MLATs as an efficient instrument for cross-border cooperation is a common theme that appears in arguments surrounding unilateral compulsion of service providers to disclose user data, and parties to this debate appear to have conflicting views on their value. For instance, while the U.S. and U.K. government agencies seem to generally complain of their unsuitability faced with the large volume and immediate nature of online threats, the Irish government seems confident of the efficiency of the U.S.–Ireland MLAT system, and the

354 For instance, the U.S. deputy assistant attorney general's testimony before a Senate hearing on law enforcement access to data stored abroad represents such a perspective: «The impacted [by the Second Circuit decision allowing Microsoft to not disclose user data stored in Ireland] investigations run the gamut – from child exploitation and human trafficking, to firearms and drug smuggling, to tax fraud, computer fraud, and identity theft. These cases directly affect public safety and may even affect national security. While the most obvious impact of the Microsoft decision may be to frustrate investigations of foreign nationals targeting U.S. victims, these examples make clear that the Microsoft decision also thwarts or delays investigations even where the victim, the offender, and the account holder are all within the United States.» B. WIEGMAN, *Statement of Brad Wiegman U.S. Deputy Ass't Att'y Gen. before the U.S. Senate Subcommittee on Crime and Terrorism*, cit., p. 6.

355 *Brief for the United States* in *U.S.* v. *Microsoft*, 6 December 2017, p. 43 (https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf).

356 *Id.* p. 52.

357 *Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as amicus curiae* in *U.S. v.* Microsoft, 13 December 2017, p. 11 (https://www.supremecourt.gov/DocketPDF/17/17-2/23693/20171213140104710_17-2%20-%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland.pdf).

European Data Protection Board (EDPB) seem to consider MLATs to be central to the GDPR's framework for data transfers to third countries in the context of law enforcement cooperation.[358]

Thus, the sense of urgency produced by a securitization posture regarding private data flows and the perceived inefficiency of bilateral cooperation agreements may create a motive for unilateral claims to prescriptive and enforcement jurisdiction, or push governments to advocate in the domestic and international level jurisdictional rules that make use of effects-based connecting factors rather than data (and/or processing) location-based ones. In this context, rules that assign prescriptive jurisdiction based on nationality or residency of the user may be interpreted to contain an assumption that communication originating from these persons have some effect on the territory and subjects of the state by virtue of the connections these persons have with the state and its society.

It should not be surprising that in determining an extraterritorial jurisdiction "strategy", governments consider international "political" costs of their choice, which are typically envisioned as a scenario of reciprocation of the strategy by foreign states. In the context of cyberspace, the tension between states' capacity to engage in unilateral action with impunity and the potential benefits of an international rule-of-law has been a treated as important issue in since the beginnings of "cyberlaw" scholarship.[359] However, in relation to digital markets, the securitization of data flows bring with it demands for alignment between international trade strategies and national security strategies, which is not very conducive to achieving a solution based on wide international cooperation.[360]

(2) Facilitation of global market access: Admittedly at this point I can only offer circumstantial evidence regarding the existence of a coherent conception of facilitation of global market access as a governmental interest to be taken into consideration when the administration or courts decide on the exercise of extraterritorial prescriptive jurisdiction, *distinct from the customary*

358 Cf. *Brief for the United States in U.S v. Microsoft*: «to the extent that an MLAT covers the requested data in a particular case, the process can be slow and uncertain, often taking many months or even years to generate results» (pp. 44-45)*, Brief for the Government of the U.K in U.S v. Microsoft as Amicus Curiae.* (see relevant quote above in text), *Brief for Ireland in U.S v. Microsoft as Amicus Curiae*: «Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime and is ready to consider, as expeditiously as possible, a request under the MLAT, if and when it be made.» (p. 8), and EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018: «In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.» (p. 5, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en)

359 M. HILDEBRANDT, *Extraterritorial Jurisdiction to Enforce in Cyberspace?: Bodin, Schmitt, Grotius in Cyberspace*, in *UTLJ*, 2013, p. 196.

360 In the context of cloud computing services, one factor leading to such an alignment may be the national security implications of powering governmental and public services with private cloud computing services. E.g. see V. KUNDRA, *Federal Cloud Computing Strategy*, 8 February 2011, (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf). In the U.S.A., this demand for alignment manifests itself in discussions regarding extraterritorial prescriptive jurisdiction in the form what I call the "bad state" reciprocity paradox. Simply put, the "paradox" arises from asking the question of «would we like if the governments of [insert "bad state" of choice] asserted their jurisdictional authority in the same way?" for each possible solution for exercising jurisdiction in cyberspace and reaching the answer "no" each time. Even a pure territorial solution based on data location cannot escape the paradox, as «that would create data havens for malign activity».

deference shown to the foreign state's sovereign right of regulating commerce in its own territory.

Nevertheless, at least in the context of the U.S., there seems to exist a doctrinal basis to consider such an interest, if found to exist, in to the international comity consideration regarding the extraterritorial application of U.S. law.[361] It has been observed that courts, including the U.S. Supreme Court have considered the United States' interest in deferring to foreign law by way of the doctrine of comity for the sake of «harmony […] needed in today's highly interdependent commercial world».[362] Also, it is stated in the Restatement (Third) of Foreign Relations Law, which compiles a review of and comments on the valid American common law in matters related to foreign relations including prescriptive jurisdiction, that in deciding whether a state (or the federal government) may exercise prescriptive jurisdiction a court will evaluate, *inter alia,* «the importance of the regulation to the international political, legal, *or economic* system».[363] Perhaps more significantly, the comity analysis prescribed in the Cloud Act itself, which will be undertaken by the court upon a motion to quash filed by the provider, stipulates that the court shall take into account, *inter alia* «the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider.»[364] Moreover, the Cloud Act requires foreign states to «[demonstrate] a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet» in order to be eligible for entering into an executive agreement with the U.S. government that would authorize that state to order U.S. service providers to disclose certain user data to their law enforcement authorities and would make them eligible for benefiting from the comity analysis prescribed in the Act.[365]

Concerning the particular context of cloud service provision and export, it appears that the U.S. government perceives conflict of laws as an important barrier for U.S. companies to exploit global markets. The U.S. Department of Commerce has assessed foreign law compliance issues,

361 Although not directly relevant to the question if prescriptive jurisdiction, this point is further evidenced in the field of personal jurisdiction. Recent U.S. Supreme Court decisions in *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915 (2011) and *Daimler AG v. Bauman* 571 U.S. ___ (2014) have effectively shifted the focus of the criteria required for a court to claim general personal jurisdiction over a transnational corporation from the degree of commercial presence a corporation has within the territory of a state *objectively* determined, to the degree of presence *subjectively* determined, i.e. presence relative to the overall size and organization of the company itself. The result is that a very large transnational corporation can escape general personal jurisdiction of a court even in cases where its operations in the forum state are worth billions of dollars. The main aim behind this change is shielding large multistate (or multinational) corporations from forum shopping, thus enabling them to enter foreign markets without attracting litigation risks in the forums of that market, except in cases where the dispute arises from the activity located in that host state, and only for damages that are suffered in that host state. General personal jurisdiction under this scheme is only allowed in the residence or headquarter of the corporation, and in practice companies can manage litigation risk through intelligent corporate structuring and by objecting jurisdiction on the basis of *forum non conveniens*. The overall result is that the adjudicatory powers of the state (and the access to justice of potential plaintiffs) are curtailed for the benefit of enabling easier market access for corporate subjects.

362 *F. Hoffmann-La Roche Ltd. v. Empagran S.A*. 542 U.S. 144, 164–65 (2004).

363 AMERICAN LAW INSTITUTE, *Restatement (Third) of Foreign Relations Law of the United States*, § 403 (1987, October 2017 Update), (emphasis added).

364 18 U.S.C. §2703(h)(3)(C).

365 18 U.S.C. §2523(b)(1)(B)(vi).

including particularly data transfer and data localization requirements as the primary international competitiveness issues facing U.S. cloud computing service providers:

> «Key International Competitiveness Issues
> When entering or expanding into international markets, U.S. cloud service providers might face some of the following market challenges:
> 1)Data localization restrictions requiring data to be stored, processed or handled in the same country where it originated.
> 2)Compliance with foreign laws establishing measures regarding how certain data maybe transferred across borders.
> 3) Being required to have a local presence in-market (e.g., distributor, sales office, business representative, joint venture partner, etc.) could make a significant difference in a company's abilities to do business, especially with the public sector.
> 4) Other competitive ness issues such as licensing requirements, and cyber security and restrictive procurement policies.»[366]

(3) Protection of the privacy rights of subjects: Although an important interest of the state, this interest is not directly relevant to the question of deference to foreign law in the context of the comity-upon-request framework of the Cloud Act. However, the foreign state's interest in the protection of the privacy rights of its citizens and residents plays a direct role in the comity assessment. The consideration of privacy rights of subjects may also be indirectly relevant in a comity analysis if the "political" consequences of exercising extraterritorial prescriptive jurisdiction are (somehow) taken into account, e.g. the foreign state reciprocating by ordering service providers to disclose data of users resident in the first state. This issue will not be detailed in this paper.

(4) IT protectionism: This interest does not play a role from the perspective of the U.S. due to the already dominant position of U.S. service providers (and the weak competition these providers face from foreign providers in the U.S. market), however for other governments protecting domestic providers from the complete domination of their national markets by foreign providers may be a real motivation which could lead the passing of privacy laws that encourage or require data localization as a matter of fact, if not by law, benefiting domestic providers in the process.[367] Nevertheless, protectionist motivations may be also thought as overlapping with the securitization trend and the facilitation motivation discussed above, as foreign domination of the domestic market could make it difficult for domestic service providers to thrive, and foreign control of a large volume of citizen (and public) data may be perceived as a security threat.

How a protectionist interest may interact with the law of jurisdiction, especially in legal systems which ostensibly reject openly protectionist trade policies is must play an important part in any theory of how globalization in computing/data services are affecting the use of conflict of laws

366 U.S. DEPARTMENT OF COMMERCE INTERNATIONAL TRADE ADMINISTRATION, *2017 Top Markets Report Cloud Computing Sector Snapshot*, p. 2, (https://www.trade.gov/topmarkets/pdf/Sector%20Snapshot%20Cloud%20Computing%202017.pdf).

367 For a recent example, see V. GOEL, *India Pushes Back Against Tech 'Colonization' by Internet Giants*, NYT Online, 1 September 2018, (https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html?action=click&module=Top%20Stories&pgtype=Homepage).

doctrines. However, as this paper is focused on the use of the particular use of comity in the Cloud Act, the protectionist motive will not be discussed in detail.

6. It has been suggested by various commentators that the fundamental reason that causes data location to be a problematic connecting factor is that in the case of data (as opposed to physical things or persons) location does not correlate with the existence of legitimate interests of the state governing that location to an extent sufficient enough to justify the exclusive prescriptive authority of the state in question regarding the regulation of the behavior related to that data.[368] It appears in the light of recent legislation and official commentary either side of the Atlantic that there is a divergence on the acceptance of this idea, at least in the policy making level. In the U.S., the recently passed Cloud Act provides for an unusual framework for international cooperation that envisions both executive-level international cooperation and collaboration between transnational service providers and (foreign) law enforcement. This framework acknowledges that deference to foreign law is inevitable to uphold the existing global data flows and value chains created by these, but it is also firm in its adoption of the idea suggested above.

On the other hand, in Europe, the recent entry into force of the GDPR with its strict rules for data transfers to third countries and extensive claim to prescriptive jurisdiction seems to represent a maximalist approach to prescriptive jurisdiction that rejects complete irrelevancy of data location as proposed by the abovementioned view. It appears that in current EU data protection law, the location of data is thought to correlate with a bundle of core interests that are protected by the most hallowed of norms, *viz.* the sovereign's right to non-intervention, and the user's fundamental right to privacy. Moreover, the from the perspective of EU law, the unfettered enjoyment of the latter right and the Union's interest in upholding it justifies extraterritorial application of EU law – this time by way of the user's residence as a connecting factor. The line, however, is drawn at extraterritorial enforcement, which represents a more traditional understanding of the difference between prescriptive jurisdiction and enforcement jurisdiction in the context of international law.

On the day of the entry into force of the GDPR, two Guidelines were adopted by the new European Data Privacy Board that replaced the Article 29 Working Party. Unsurprisingly, both concerned transfer of data to third countries. The second, Guidelines 2/2018, directly foreclosed the possibility that Article 49 could provide a basis for cooperation of the data controller with third country law enforcement, a possibility that was suggested by the European Commission in its amicus brief in *Microsoft*:[369]

368 E.g. see J. DASKAL, *Borders and Bits*, in *VLR*, 2018, p. 226; D. SVANTESSON, *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, AJIL Unbound*, 2015, p. 72. For a view arguing that territory never had much representative power regarding state interest see P. D. SZIGETI, *The Illusion of Territorial Jurisdiction,* in *TILJ*, 2017, p. 371.

369 «The legitimate interest [under GDPR art. 49(1)] could, again, be the interest of the controller in not being subject to legal action in a non- EU state» *Brief of the European Commission on Behalf of the European Union as Amicus Curiae in U.S. v. Microsoft*, 13 December 2017, p.16, but also «It should also be noted, however, that Article 49 is entitled "Derogations for specific situations." Therefore, these grounds are to be interpreted strictly» (ibid. at 17) (https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

> «The GDPR introduces a new provision in Article 48 that needs to be taken into account when considering transfers of personal data. Article 48 and the corresponding recital 115 provide that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries. Therefore, a transfer in response to a decision from third country authorities is in any case only lawful, if in line with the conditions set out in Chapter V. […] In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), *EU companies should generally refuse direct requests* and refer the requesting third country authority to existing MLAT or agreement.»[370]

Similarly, an amici brief for MEPs in *Microsoft*, whose *amici* includes Viviane Redding, the EU commissioner that initiated the legislative work for the GDPR, and Jan Philipp Albrecht, the parliamentary rapporteur for the GDPR and the U.S.-EU "Umbrella Agreement", took a strict view of the exclusivity of the Art. 48 rule requiring an international agreement basis for data disclosure to third country law enforcement organs and categorically denied the applicability of the Article 49(1) "important reasons of public interest" exception to disclosures to foreign law enforcement.[371]

This difference in views poses a problem for transnational service providers which deal in very large volumes of transatlantic data transfers. As purveyors and movers of data and storage thereof, it appears that it would be more in the interest of service providers if data location would not be representative of the existence of such a bundle of core governmental interests. As a significant feature of their business models and economies of operation depends on global transfers of data, it can be conjectured that the less a change in data location signifies a change in corporate legal obligations, the better it is for the corporation. On the other hand, if it is not possible to completely disassociate governmental interest from data location, another beneficial option would be curtailing extraterritorial application to avoid conflicts of law for the sake of foreseeability. Both configurations can theoretically be achieved through international intergovernmental cooperation, but the latter configuration may also arise through unilateral actions of states under certain circumstances where governmental interest is found to be best served with prescriptive self-restraint.

States are jealous of their prescriptive powers, and they will not forfeit them lightly. States may voluntarily limit their extraterritorial prescriptive powers when they recognize an interest in deferring to the sovereign rights of other states, notwithstanding the theoretical legal problem of whether there is a norm of international law that require them to do so. For example, it seems that the United States courts recognizes an interest in upholding the «highly interdependent global market» by refusing to apply U.S. law in cases where legitimate foreign interests call for the application of foreign law, or by deferring to private choice-of-law or arbitration agreements at the

370 EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, cit., p. 5 (emphasis added).

371 *Brief of amici curiae Jan Philipp Albrecht, Sophie In'T Veld, Viviane Reding, Birgit Sippel, and Axel Voss, members of the European Parliament* in *U.S. v. Microsoft*, 18 January 2017, p.17, (https://www.supremecourt.gov/DocketPDF/17/17-2/28328/20180118155453076_17-2%20bsac%20Jan%20Philipp%20Albrecht.pdf).

expense of the authority to enforce public policy.[372] Although the issue is far from settled in U.S. law, it is notable that in his amicus brief in *Microsoft*, the U.N. Special Rapporteur on the Right to Privacy seemed to espouse the view that considered deference to the foreign law via the doctrine of international comity as a requirement of fostering commercial relationships between nations, citing the *Empagran* decision:

> «Respect for foreign sovereigns is not, however, premised solely on an abstract notion of sovereign independence. Rather, it is a practical element of fostering positive diplomatic and commercial relationships between nations and preventing "international discord." Nor is comity solely the concern of the judiciary. As this Court observed in F. Hoffmann-La Roche Ltd. v. Empagran S.A., it is assumed "that legislators take account of the legitimate sovereign interests of other nations when they write American laws, [which] helps the potentially conflicting laws of different nations work together in harmony – a harmony particularly needed in today's highly interdependent commercial world." Executive agencies are similarly expected to consider the interests of foreign sovereigns when enforcing domestic laws.» [citations omitted][373]

7. A common theme found in critiques of the Court of Appeals for the Second Circuit's decision for Microsoft[374] (which was appealed to the Supreme Court and had found that the FBI's use of the disclosure warrant was indeed extraterritorial based on data location and therefore unlawful) and Microsoft's pure territorialist views on data location and prescriptive jurisdiction is the argument that data location does not serve as a good proxy for the state interests involved in the dispute, rendering the use of data location as a connecting factor a bad conflict of laws practice. At the core of this argument is the premise that all connecting factors, especially those that are based on the notion of territoriality, are proxies for certain preferred stratifications of the interests (of relevant parties, sovereigns, and third parties) being affected by the legal event in question. According to this, rules concerning adjudicative, prescriptive and enforcement jurisdiction all operate through concepts that encapsulate the postulated interests of actors. Examples are territory of a sovereign, nationality of an actor, location of an immovable, place of contracting, using a satellite uplink, advertising in a certain language, participating in a commercial fair. In other words what these kinds of factors and concepts achieve is to allow courts to favor the interests of one party (or sovereign, or third party) over another by simply making a binary choice as to the existence of the connecting factor, thus keeping the question strictly within the sphere of legal analysis, by

372 *F. Hoffman-La Roche, Ltd. v. Empagran, S.A* 542 U.S. 155 (2004) cited in J.R. PAUL, *The Transformation of International Comity*, in *LCP*, 2008, p. 36. Paul critiques the development of the doctrine of international comity in U.S. courts and argues that it is increasingly used to relinquish state authority to prescribe public policy not only in deference to foreign sovereigns, but more importantly in deference to the global market itself.

373 *Brief Amicus Curiae of U.N. Special Rapporteur on the Right to Privacy Joseph Cannataci in Support of Neither Party* in *U.S. v. Microsoft*, 13 December 2017, pp. 32-33, (https://www.supremecourt.gov/DocketPDF/17/17-2/24918/20171222120327043_35632%20pdf%20Krishnamurthy.pdf)

374 *Microsoft Corp. v. United States*, 2nd Cir., 14 June 2016, vacated by Supreme Court as *United States v. Microsoft Corporation,* 584 U.S. ___ (2018).

having the court not to engage into a technical discussion of all the interests at stake in the conflict and stratifying them, which is a political action in nature.

For instance, when a court decides that the law of country X applies and not country Y, because the performance of the contract provision in question was to take place within the territory of country X, the conflict rule that the court is applying, i.e. that the law of the place of performance of the contractual obligation will apply, solves the balancing of interests problem by reducing the question of competing interests to a relatively less controversial, less complex, and much more easily observable factual finding that the court can make based on much less evidence and technical expertise compared to actually identifying and calculate the interests at play. The binary choice (existence or non-existence of performance obligation in X or Y) essentially provides two scenarios in which the stratification of interests are "pre-calibrated" by the legislator, e.g. in our scenario of the contract, it is decided by the legislator *ex ante* to the dispute that the interests of the state in whose territory the performance will take place trumps that of the state which is connected to the legal relationship in other ways, with regards to the regulation of the contract. The pre-calibration of this preference for the interests of the state in whose the territory the contract is performed is applied generally and may include cases in which the normative concerns of the legislator would actually point to the other state's law to be applied, but the benefits of the general rule is assumed to outset the occasional misappropriation. The view that such *ex ante* pre-calibration is prone to error in and is essentially arbitrary has formed the basis of what is called the American Conflicts Revolution, and the rise of "governmental interest analysis" as an alternative *ex post facto* interest stratification method for courts to choose the applicable law in the United States.[375] In Europe, where active interest analysis by the courts was theoretically undesirable due to its political nature, courts have nonetheless used *ordre public* exceptions and other escape mechanisms included in the system based on the pre-calibrated rules to bridge cases in which they thought the conflict of laws rules yielded misappropriation.

The proxy theory is compatible and favorable to the hypothesis propounded in this work, that there is an informational problem that underlies the development of the "privatizing" solutions in global data flow regulation, and in particular, the *comity-upon-request* regime brought by the Cloud Act in the U.S. The informational problem is more acute if it is assumed that facilitating or ensuring global market access for domestic capital has become a central interest of the State. This would mean that determining the state's interests in a conflict case now (to a much greater extent) entails assessment of market responses to the global regulatory reach of the of the State. In the context of data flows, such assessment increasingly requires specialized technical knowledge and insights because of the rapidly changing and disruptive nature of the technology sector. Courts no longer can rely on proxy concepts to make an interest analysis that can properly account for the State's interest flowing from its new role. They simply lack the information, and the application of the former proxies can lead to unintended results. Thus, the solution to this problem is to "outsource" the information gathering to the corporations that can avoid rules that are "counterproductive" in the light of the State's new central interest through choice of law, choice of forum, or arbitration agreements; but now even in the field of regulation that is based on public policy, it appears that States may allow transnational companies to make decisions about the

375 S. C. SYMEONIDES, *The American Choice-of-Law Revolution: Past, Present and Future*, cit.

regulatory reach of the state according to the information they have from their commercial operations, as it will happen under the Cloud Act's comity framework. Corporations then can have a say on whether the application of public policy would be beneficial or not on their own information on the possible effects of a conflict.

It is in this sense that data is different because it no longer serves the courts (but also the legislators) as a proxy for public policy – the regulation of a located thing according to the territory that it is located in makes sense insofar as the regulation of such thing serves in some way the interests of the state, such as the distribution of resources among the members of a located populace. But when the role of the state is providing the members of that populace access to the markets that distribute the profits generated from the processing of that thing, which in the context of data entails its continuous movement and global flow, the State's interest in regulating such thing is decoupled from the location of that thing, as there is no nexus left between the location of the thing and the benefits expected from its regulation.

Let us exemplify what is said here by reference to the provisions of the Cloud Act. Let us assume that the U.S. law maker has in its focus two competing interests (as I have argued above is indeed the case) namely securitization of private data flows and the facilitation of global market access for U.S. service providers. Data location is not a connecting factor conducive to the efficient protection of both these interests. According to §2703(h)(2)(A)(i), the comity-upon-motion option is conditional on the provider's reasonable belief that the target user is not a United States person *and* does not reside in the United States. Upon motion to quash, the court will ensure that this is the case before making a comity analysis. This provision effectively locates the focus of state interest in the close connection between the user and the state, rather than connection between the service (data storage) and the state. Data location, that suggests the latter type of connection, is not rejected completely as a valid ground for prescriptive jurisdiction, but can be overridden via comity analysis when the U.S. service provider risks "penalties"[376] due to the conflict of laws. This is in line with the state's facilitation interest. On the other hand, by foreclosing the comity analysis for disclosure orders regarding U.S. persons, the law basically provides for an effects jurisdiction rule with an irrefutable assumption that activity of U.S. persons and persons located in the U.S. will always be directed to the U.S, as the security interest of the state requires that procedural and substantive rights under foreign laws should not be invoked to limit the jurisdiction of American courts and lawmakers in cases where the effects of the activity is directed towards the U.S. It cannot be asserted that the law tries to uphold the jurisdiction of the natural judge of the user, as jurisdiction to issue a warrant in any case lies with the court of the judicial area in which the crime or activities related to the crime have occurred (Federal Rules of Criminal Procedure, Rule 41(b)(6)).

8. This paper sought to argue that the *comity-upon-request* framework provided in the new U.S. Cloud Act is a partly a result of the U.S. government's motivation to facilitate global market access of its domestic cloud computing service providers. To achieve this goal, an "information problem" as I have explained in this paper must be overcome, and I have argued that the comity analysis solution provided in the Cloud Act has been shaped to solve this information problem by shifting the job to determine and address conflicts of laws to the service providers. Through this

376 18 U.S.C. §2703(h)(3)(C).

authority, service providers now have a say in whether and when the exercise of extraterritorial prescriptive and enforcement jurisdiction is acceptable, a job that is traditionally within the exclusive competence of state organs, since it is typically considered to be a function of sovereignty.

My findings are dependent on two assumptions to be inferred properly. First, there must be an identifiable state interest of facilitating global market access, and this interest should be able to clash with other traditional state interests so that a novel jurisdictional rule that takes into account the information problem would be needed. Second, data location based territorial rules should be unable to meaningfully distribute authority between states in a way sensitive to the clashing state interests I have identified in my assessment of the first assumption. In this paper, I sought to provide evidence and observations to support these assumptions, and thus justify my inferences about the form of the new comity framework.

KAYAHAN CANTEKIN
European University Institute (EUI)

II.3

Digital evidence for the criminal trial: limitless cloud and state boundaries

SUMMARY: 1. A baffled king. – 2. Mutual Legal Assistance and its shortcomings. – 3. The Empire strikes back: national remedies. – 4. Finding effectiveness: an EU regulation proposal. – 5. Conclusions.

1. It is hard to find a stronger manifestation of state sovereignty than the power to investigate a crime, try the suspect for it, and punish him once he is found guilty. The whole process is a show of public force: it brings reluctant witnesses to the stand, forcing them to tell the truth; it can violate the privacy of an apartment or listen to a phone call. In the last decade, another tool has been gaining importance on the criminal trial's stage: the sheer amount of data we produce daily can tell a lot about what we are up to, and it is no wonder that it can come handy during the investigation of almost any crime. There is no need for a cybercrime, or for the misuse of a device: digital information can always be relevant. The list of the last locations of the victim, the name of the person s/he was texting with, the record of a phone call or an email; all this data could play a role in any investigation.

This type of evidence, however, differs substantially from something as mundane as a knife: we share a significant amount of information with the company that provides the service to us[377]. They gather almost everything we produce and store it on a server[378]: we can access the information whenever we like, but it is physically preserved in a data center at the other corner of the world, displaced from time to time to ensure the efficient use of the infrastructure[379].

377 A couple of examples: the Onion – a satire U.S. website – described Facebook a C.I.A. program, and the most effective one. Since then, the company has gained access to more information developing a facial recognition algorithm, sharing the information among devices, so that it can keep track of phone calls and text messages sent outside the platform. However, Facebook is not the only one: Tinder – the dating app – keeps scrupulous records of all the users to improve the matching algorithm. A journalist asked for her entire record and received a staggering amount of data regarding her preferences: see J. Duportail, *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*, in *theguardian.com*, September 26, 2017.

For a strong critique of the *status quo* and technological ways forward see: S. Rasmussen, *The BINC Manifesto: Technology driven societal change, science policy &stakeholder engagement*, in C. Gershenson, T. Forese, J. M. Siqueiros, W. Aguilar, E. J. Izquierdo, H. Sayama (eds.), *Proceedings of the Artificial Life Conference 2016,* at *turing.iimas.unam.mx*; M. Monti, S. Rasmussen, *RAIN. A Bio-Inspired Communication and Data Storage infrastructure*, in *Artificial Life,* 2017, p. 552-557.

378 Sometimes it is a service; some others it is a business model: acquiring and selling data has become a business of its own, and according to the documentary *Terms and conditions may apply* (2013), it began with the Patriot Acts, that required the big tech companies to store information for surveillance purposes. Then they realized they could make money off of the incredible haystack they were building and started to do so.

For other industries, gathering data is vital to maintain the product working: artificial intelligence, for instance, needs to learn from past examples. Without memory, it cannot function, so it needs to keep a considerable amount of information to calculate the next answer.

379 See J. Spoenle, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, August, 31, 2010, *rm.coe.int*; for a technical explanation, see Y. Sahu, R. K. Pateriya, R. K Gupta, *Cloud Server Optimisation with Load Balancing and Green Computing Techniques Using Dynamic Compare and Balance Algorithm*,

Long story short, those data have an owner: often a big, powerful one that operates on an international level day in and day out. The company does not need to be located or even represented in a country to provide services within its boundaries, and it is free to set up branches of their organization wherever they want, according to the most convenient business strategy.

This scenario is enough for traditional categories to lose their focus: citizenship and sovereignty can be set aside with ease, whereas the private policies of a single company can have a transnational impact[380].

On the one hand, being a citizen means enjoying a certain set of rights, which does not necessarily apply to one's data once they transit over a foreign server[381].

On the other hand, the authority of the state is not enough to gain access to the information produced on its own soil, relating to a crime entirely carried out on its territory. It is somewhere else, out of its reach. Law enforcement authorities have to ask for the help of the competent state through the available Mutual Legal Assistance (MLA) tools, and not because of the transnational nature of the crime: as we already mentioned, that could be entirely carried out within a nation's territory. Digital evidence, however, follows the fragmented, international territoriality of providers; not the political boundaries set to national states.

Given this framework, we will rapidly point out the main flaws of the traditional system and how some European states have been developing a different approach to secure the evidence anyway. Then, we will focus on a proposal for a European regulation that faces the issue, aiming to introduce new possibilities of direct interaction between states and service providers.

2. When the state cannot secure the necessary information on its own, it can ask for help: every nation has its arsenal of tools and procedures to obtain the assistance of the competent state, generally based upon a patchwork of bilateral or multilateral treaties. The procedures that they provide for, however, are often cumbersome and slow, which is especially problematic for a kind of evidence that can be quickly erased, modified, encrypted or displaced[382].

Within the European Union, the cooperation should be simplified by the brand new European Investigation Order (EIO), in an attempt of standardizing and expediting the procedure; nonetheless, it does not contain any specific provision on digital evidence, focusing only on spot operations like the identification of the person "holding a subscription of a specified […] IP address"[383].

in *2013 5th International Conference and Computational Intelligence and Communication Networks, IEE Xplore*, 11 November 2013.

380 For a vivid example, see R. Budish, H. Burkert, U. Gasser, *Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects*, May 2, 2018, in cyber.harvard.edu.

381 See *Terms and conditions may apply* (2013) on the Total Information Awareness program; see *Citizen four* (2014) on the NSA domestic surveillance programs, based upon the documents leaked by Edward Snowden and subsequently made available by the N.S.A. itself, on the web page of the Domestic Surveillance Directorate: nsa.gov1.info.

382 For further considerations on the topic, see A. K. Woods, *Against Data Exceptionalism*, in *Stanford Law Rev.*, 2016, p.749.

383 Art. 10, lett. *e* of the directive; the Italian transposition added to this list also the identification of the person behind an email address: art. 9 lett. *e* D.Lgs. June 21, 2017, n. 108.

Moreover, Ireland is not a party to the directive, so it has not transposed it nor can be bound by its provisions, and this could be a major problem: most of the big tech corporations have their the European headquarters there. As a result, the ordinary MLA procedure is to be adopted, which means at least that the competent central authority has to be involved in the transmission of the request. The same applies to requests directed to non-EU countries such as U.S. and Canada.

Another problematic step is the phrasing of the request, that should be as specific as possible, so that the competent authority can decide what to do with it. It is tricky for all kind of requests, but the dialogue about digital evidence can be further complicated: there is no shared legal definition about the type of data that can be demanded, and no shared understanding of the conditions under which a certain kind of information can be released. The lack of common grounds can hurt the communication and a request – complete under the law of the issuing country – can be discarded as unbearably generic by the recipient[384].

Once the application is ready, one must decide to whom it shall be addressed, and it is no easy step. Which is the competent state to deal with it? The country where the company is based? The country where a local branch is based? The country where the data are stored? Each law can locate the provider according to different criteria, and as a result, there is little or no clarity as to who can obtain the information[385]. Providers as well hold their views as to which country has the authority to compel the production of their records, agreeing spontaneously to some requests and fighting others[386]

The best shot of the issuing authority is to forward the request to every state that is potentially connected to the information, hoping for at least one positive answer; of course, this method is not the most efficient for both the issuing and the receiving authorities[387].

But let us assume that at least one of these requests has landed in front of a receiving authority that can actually help. The investigators should find the required data, and the best way to do that is asking the provider, but not many European countries have a transparent procedure in place to cooperate with them.

Finally, MLA requests are suddenly going from "boutique" to "fast food"[388]: the number has been increasing, and many states do not have the resources to respond to all the asks adequately. It is time and energy consuming, and there is no interest of the receiving authority at stake, which can

384 For more on the topic, see the *Commission staff working document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, April 17, 2018, SWD(2018) 118, p.* 30 and following.

According to a survey on cross-border access to electronic evidence conducted by the European Commission, another common experience is the refusal to comply with the request due to the difficulty in establishing probable cause, which is also a sign of lack of specificity; see *Questionnaire on improving criminal justice in cyberspace. Summary of Responses*, 2017, p. 5, ec.europa.eu.

385 See K. Westmoreland, G. Kent, *International Law Enforcement Access to User Data: A Survival Guide and Call for Action*, in *Canadian Journ. of Law and Technology*, 2015, p. 232.

386 A. K. Woods, *Against Data Exceptionalism*, p. 735-736 and p. 745-747.

387 See *Questionnaire on improving criminal justice in cyberspace,* p. 7.

388 A. K. Woods, *Data Beyond Borders. Mutual Legal Assistance in the Internet Age*, 2015, uknowledge.uky.edu, p. 3.

result in a time-conservative work schedule. Those requests will be answered but with low priority, which could defeat the purpose of cooperation or make it impossible: data cannot be stored forever; they could be erased or encrypted while the ask lingers on someone's desk[389].

This delay in the response is the most urgent problem to solve: a good timing has always been critical to the success of the operations but, with electronic evidence, the whole process needs to be further expedited.

Confronted with this reality, many scholars have come up with proposals to adjust and modernize the framework.

One calls for a better response from private companies, which could be victims of cyber-attacks at any time: that they should invest more in digital security and digital forensics so that they can provide data to whoever can prosecute the crime they suffered[390]. It seems to be a form of self-help though, and not a solution that could benefit the entire system: the cooperation could be smoother for attacks on some victims, leaving everyone else out.

Other proposals touch directly upon a deeper problem: is the cloud manageable at all through the territoriality principle, or is it too hard to maintain this expression of sovereignty? According to some scholars, it is time to break down the borders, since territoriality is "the main obstacle for investigating actions within the clouds"[391]. Many theories stemmed from this premise: according to one of those[392], territoriality should be adapted to the challenges of a globalized world, or, at least, it should apply just to the jurisdiction, but not to the investigation. The cross-border access to digital evidence would then been ensured. This idea, however, could be hard to sell to the states themselves: they should allow a foreign authority to carry out an inquiry on their soil[393], which does not seem a realistic expectation. Moreover, the proposal would be of some use while following a live communication, but not as much in asking a private company for stored data, which seems to be the main issue[394].

Others have been trying to make territoriality more manageable, for instance by searching for a more tangible connecting factor: the location of the data can bring to inconsistent results, and it is difficult to establish. It should be replaced by something easier to ascertain as the formal power of disposal of the information[395]

Finally, it has been argued that digital information is not so special after all: it is stored on a physical layer that permits – among other criteria – to establish jurisdiction according to the

389 According to *Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies*, December 12, 2013, in obamawhitehouse.archives.gov, p. 227, "requests appear to average approximately 10 months to fulfill". Since the report, the number of MLA request directed to the U.S. has more than doubled: see A. K. Woods, *Against Data Exceptionalism*, p. 750.

390 J. I. James, *How Business Can Speed Up International Cybercrime Investigation*, in IEEE, 2017, p. 105.

391 J. Spoenle, *Cloud Computing and cybercrime investigations*, p. 8:

392 D. J. B. Svantesson, *Law Enforcement Cross-border Access to Data*, 2016, in researchgate.net.

393 J. Spoenle, *Cloud Computing and cybercrime investigations*, p. 10.

394 J. P. Mifsud Bonnici, M. Tudorica, J. A. Cannataci, *La regolamentazione delle prove elettroniche nei processi penali in "situazioni transnazionali": problemi in attesa di soluzioni*, in M. A. Biasiotti, M. Epifani, F. Turchi (a cura di), *Trattamento e scambio della prova digitale in Europa*, Napoli, 2015, p. 213.

395 J. Spoenle, *Cloud Computing and cybercrime investigations*, p. 10-11.

territoriality principle, allowing the whole structure to function[396]. The MLA system, nonetheless, would need a serious restyling to improve the response time and improve efficiency[397].

3. Given the intricacies of the MLA, States have come up with different approaches based on unilateral action, to obtain access and avoid the pains of cooperation with foreign authorities altogether. The individual strategies can be more effective, but that can also imply a big price to pay for the companies or the rights of the user.

The most infamous shortcut is mass surveillance, which impacts disproportionately on the individual's right to privacy. Other methods can protect the people and the national interest to access evidence, but strongly affect the liberties of the service providers: some states ask (or have considered asking) to locate all relevant information within the borders, so that it can be accessible at all time.

We will not delve into these attempts; instead, we will analyze the different strategies put in place by France, Germany and Italy. All those countries share the same need, but do not adopt the same approach in dealing with it.

France, for instance, is one of the few countries in the European Union to have explicit legislation in place that allows for the direct cooperation between law enforcement and service providers, and it has been there for quite some time. In 2004, art. 60-2 was introduced in the Code of Criminal Procedure, offering a legal base for direct cooperation with service providers[398]. Although it is limited to a particular kind of inquiry (*enquête de flagrance*), it serves as a model to the other provisions enabling such joint effort also in the other types of investigation that the Code describes: it is the case of art. 77-1-2 for the *enquête préliminaire* and art. 99-4 for the *instruction.*

This system contains two main possibilities: first, the providers have to disclose all the "information that is useful to the manifestation of the truth", unless they can oppose a privilege recognized by the law. The provider has to respond within the shortest delay possible; if it fails or refuses to answer without a legitimate motive, it will receive a 3.750 euro fine. Second, the law enforcement authorities can also require a specific class of service provides – those hosting communications over the internet – to preserve content information for up until one year; to do that, a judge has to review the application.

The requests are subject to the procedure that the regulatory part of the Code lays out. They ask the police to write a detailed report on the ask, specifying which company has been asked and what kind of information are to be handed over. As to the practical details of the interaction, they are established by a protocol approved by the ministry of justice and every organization with which the law enforcement needs to cooperate.

396 It is the main argument of A. K. Woods, *Against Data Exceptionalism*, to which responded D. J. B. Svantesson, *Against 'Against Data Exceptionalism'*, in *Masaryk University Jour. of Law and Tech*. 2016, p. 200; as well as Z. D. Clopton, *Data Institutionalism: A Reply to Andrew Woods*, *Stanford Law Rev. (online),* 2016.

397 For a multi-dimensional approach, see A. K. Woods, *Data Beyond Borders*, p. 8-14. The same view has been held by DigitalEurope, *DIGITALEUROPE views on Law Enforcement Access to Digital Evidence*, October 17, 2016, p. 4: the document encourages a more efficient MLA remedies instead of unilateral actions to access cross-border evidence.

398 Art. R15-33-68 contains the list of what enterprises are to be considered service providers for the purposes of this statute.

So, when the state asks for information, the request is regarded by the state as binding: not answering is punished with the fine but also with a class II misdemeanor, for disobeying the orders of a court of law[399]; both the punishments, however, can be easily factored in the decision not to answer: the criminal misdemeanor is punishable with another fine whose maximum amount is 150 euros. Moreover, those rules do not seem to apply to a service provider that is not established in France, or, in any case, it is not clear how they could be enforced without the cooperation of another country[400], which leads us back to square 1.

The system, however, seems adequate to interact at least with domestic providers, even if the deterrence of the sanctions is quite low. This mechanism relies heavily on the voluntary cooperation of the service providers but does not solve the main issue: the state does not have means to coerce compliance, if necessary.

The approach has not been shared by Germany, that has recently passed a new law addressing the issue of illegal content spreading through social networks (*Netzwerkdurchsetzungsgesetz – NetzDG*)[401]. This piece of legislation, among other things, asks all social networks to choose a representative that operates within the territory of the state: he or she will be in charge of dealing with the (criminal) law enforcement authorities' demands; the company is required to disclose the information within 48 hours upon receipt[402]. The style here is radically different. What Germany has done is forcing the providers to establish a direct, visible connection between the country and the platform, so that the state can have an easy access point and start the procedure quickly and officially. Unlike the French regulation, it gives a precise deadline to the companies, under the penalty of 500.000 euros for the failure to respond[403]. The law clearly states that the infractions shall be punished even if they are committed abroad. The aim is clear: it is about getting back territoriality (so, sovereignty) as to what happens within German borders, and the jokes are on the service provider. It is its responsibility to delete illegal content, to battle hate speech and to help to prosecute potential crimes in a short delay from the request.

399 Art. R642-1 of the French Criminal Code.

400 The survey of the European Commission showed that France is among the states that have concluded formal or informal agreements with foreign service providers and that consider the cooperation mandatory, although it is not clear what to do in case of the company's failure or refusal to respond.

401 This new statute is highly controversial. On the one hand, it has been criticized by the U.N. and the E.U. as a law allowing for censorship; on the other hand, the application of its provisions to their full extent would lead to an extra esteemed cost of 530 million euros per year: M. Etzold, *Facebook attackiert Heiko Maas*, May 28, 2017, wiwo.de.

The new law imposes to all the major social networks operating within German boundaries to delete illegal contents after 24 hours from a complaint. It is now in force since a few months and the German press already reported a general failure to respond to the illicit content. According to the reports that have been released, the compliance rate varies highly from company to company. While YouTube and Twitter try to be as efficient as they can, Facebook reportedly fall way behind the schedule, and has been criticized for how the report mechanism has been structured: F. Rütten, *Wie Facebook und Twitter das neue Löschgesetz umsetzen*, January 4, 2018, stern.de; *Facebook löschte bisher nur 362 Beiträge*, July 27, 2018, t-online.de; *Fast 500.000 Beschwerden, nur wenuge Löschungen*, July 27, 2018, manager-magazin.de; F. Steiner, *Wie viel Facebook & Co. mithilfe des NetzDG löschen*, July 27, 2018, deutschlandfunk.de.

402 § 5 (2) *NetzDG*.

403 § 4 (1) n. 8, § 4 (2) *NetzDG*.

Nothing of the kind has been happening in Italy: there is no legislation regulating interaction with any service provider, that fall under the general regulation of searches and seizures. They can voluntarily cooperate and give out the information or be searched. There has been little or no attention to specific issues, apart from some vague provisions regarding the chain of custody and the seizure by copy, which is an option available only for service providers[404]. Playing in this scenario, the investigators have two main ways to get the information they want: the first one is targeting the device[405]. It is an easy remedy, but it has two main flaws: first, the device could not be an easy access point to all the information stored in the cloud; it could be the opposite: the cloud could be an effective way to peek into an encrypted cell phone[406]. Second, the information displayed on the device is often a copy of the original, which is stored safely somewhere else: some records could be altered or canceled, undermining the reliability of the evidence. The issue here is not the admissibility in court – the rules on authentication are quite relaxed – but it is still important that the evidence collected and presented at trial has a strong probative value, which could be achieved through the transparent cooperation with service providers. Law enforcement has to rely then on the spontaneous cooperation of the providers, that can decide to answer to disclosure requests or to refuse it without fear of consequences[407].

4. The current legal framework needs to be reshaped, as it does not seem to be efficient for any of the stakeholders involved. The states cannot rely upon sure means of cooperation, and the MLA procedure does not seem to be an option (at least, not for all cases that potentially require access to digitally stored evidence). The providers are in an awkward position: they have to keep good relationships with the states they are doing business in, but they also cannot afford to disclose costumers' data without due process: the enhanced protection of privacy has been a selling point since Snowden's revelations[408]. In between, the users cannot do much more than wait and see: they agreed to terms and conditions that normally allow for any kind of appropriate action to help to

404 This is another issue that legislations struggle with: does the copy of a bunch of information amount to a seizure? In Italy yes, but just for one kind of duplicate (bit stream image): see Cass., S.U., July 20, 2017, *Andreucci*, n. 40963, in *C.e.d.*, n. 270497, for a note, see L. Bartoli, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen. (web)*, 2018, f. 1. In the U.S. it is still unclear whether or not the Fourth amendment is to be applied to the digital duplication: according to a well-known perspective, yes, but only if it is not possible to examine the data before copying it: O. Kerr, *Fourth amendment seizures of computer data*, *Yale L. Journ.,* 2010, p. 700; for an overview on the issue, see *Digital Duplication and the Fourth Amendment*, *Harv. L. Rev.*, 2016, p. 1046.

405 On the low level of protection that the device enjoys in the Italian system see G. Lasagni, *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in *NJECL*, 2018, p. 386.

406 Quite the contrary: it could be encrypted and the cooperation with the provider could be the shortest way to get ahold of the contents, as the S. Bernardino case has clearly demonstrated.

407 Facebook, for instance, has been heard on how it cooperates with law enforcement authorities to prevent hate speech and violence against women: for an example, see the Italian Senate commission on Femicide and gender related violent crimes, transcript of the hearin held on July 25, 2017, *senato.it*, p. 30 and following.

408 Amazon, for instance, has made very clear that it will challenge all the requests that deems insufficient and that it is lobbying for the introduction of adequate standards for this kind of cooperation: see S. Schmidt, *Privacy and Data Security*, June 12, 2015, *aws.amazon.com*. After all, Amazon had the largest share in the cloud services' market: see C. Coles, *AWS vs Azure vs Google Cloud. Market Share 2018*, May 1, 2018, *skyhighnetworks.com*.

investigate a crime. The decision is ultimately in the companies' hands: if they tend to be indulgent towards the requests, the information will be handed over, and often the procedure will not guarantee the basic safeguards as to the necessity and the proportionality of the investigative action.

The overall picture is nothing short of chaotic. The burden of extra-territoriality has been passed on to providers, which directly receive the requests, phrased according to different national frameworks instead of having them channeled through a single "competent authority". Together with the burden, however, comes the power to decide on a case-to-case basis: the single company can make its own policy as to the cooperation, and since it is voluntary, 'No' is always an option[409].

Thanks to a thorough consultation with States, national judiciaries, law enforcement authorities and the association of the service providers, the European Commission identified the core issues: the complete obscurity in the procedure, the lack of reliability and the troubles in holding both companies and law authority agencies accountable for their actions. To face these deficiencies, the European Commission has drafted a proposal for a regulation which – if approved – would govern and enhance direct cooperation between individual states and service providers by introducing two new tools, the European Production Order and the European Preservation Order[410].

The European Production Order is intended to oblige service providers to hand over information to the member state that requires it, without the necessary involvement of the law enforcement authorities of another member state. The European Preservation Order aims at freezing useful information, allowing the law enforcement authorities to follow through with a request to secure the evidence, neutralizing the risk of losing relevant material.

They would enlarge the spectrum of possibilities when it comes to cross-border access to digital evidence: they would not replace any MLA solution; they would just provide for an alternative. Moreover, they would not abolish per se any national solution already in place, meaning that any law enforcement authority will be able to choose how to ask for the information it needs. On the one hand, this strategy could play well, allowing a certain degree of flexibility: the investigators could be free to choose the tool that better fits into their strategies, being just able to count on two new cards in the game. On the other hand, this could bring to a residual application of the regulation: it is a compelling mechanism, but it also comes with some conditions attached. It could be easy to circumvent its limitations by simply resorting to an informal ask to the service provider: it has worked so far and could work again in the future. It looks like it is up to the private companies to uphold a single standard when it comes to this matter: they are the ones having to respond to the information requests in the first place, and they have an interest in reducing the

409 As a result, some states normally get what they want whereas some others are left behind: See European Commission, *Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, December 2, 2016, 15072/16, in data.consilium.europa.eu (hereafter: *Non-paper 1*), p. 9-10.

K. Ligeti, G. Robinson, *Cross-border access to electronic evidence: Policy and legislative challenges*, in S. Carrera, V. Mitsilegas, *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*, Brussels, p. 103. The authors remarked that the compliance rate highly varies form country to country, at least in Google's response pattern. They positively respond to the 75% of requests from Finland, but they do not respond to Hungarian authorities.

410 See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, SWD(2018) 118, April 17, 2018, eur-lex.europa.eu.

variables. Then, they would probably use the procedure as a shield: they would hand over data under a binding order, instead of passing information "under the desk", according to non-transparent policies or a case-by-case rationale.

Coming down to the details: the regulation provides for a common set of definitions as to what qualifies as a service provider and what kind of records can be secured.

Let's start with the first classification: the draft regulation mentions communication services, internet domain and IP numbering services and information society services as defined by Art. 1(1) point (b) of Directive (EU)2015/1535. This last reference is designed to include «any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services», which can apply to a broad set of situations: for instance, all the marketplace and social networks are included. The companies that provide such a service can be reached by the authorities of any member state as long as they offer their services in the European Union. In other words, they are subject to those orders if they enable physical or legal persons within the union to use the services they provide or if they have a substantial connection to the European Union; therefore, the regulation does not apply to companies that do not fall in those categories and to services that are rendered outside the European Union.

As for the type of data that can be obtained, the regulation lays down four categories: subscriber data, access data, transactional data and content data.

The first two categories are the least problematic with respect to the interference that the disclosure would realize, and they should normally be interesting at the early stages of an investigation to identify the suspect; they consist in information such as the name and address of the user; the IP address and the logs of access to the service[411].

Transactional and content data, on the contrary, are suitable to be presented as evidence as to what happened: they can be defined as metadata and the actual text message, email, photo, video, recording and so on. The treatment of these last two is much more problematic: even if the metadata does not seem as decisive, they can be interconnected with other information and help painting a pretty accurate picture of what the specific content was; however, the most intrusive measure is for sure the order to disclose content data.

For this reason, and to ensure a minimum level of proportionality, the regulation provides for two safeguards: the order to produce transactional and content data shall be approved by a judge or a court, and can be only issued if the alleged infraction is punished with a custodial sentence of not less than three years in its maximum amount.

A production order for subscriber and access data can be issued for all criminal offenses, and the authority of the prosecutor will suffice as there is no need for the validation of the judge.

The difference in treatment seems reasonable: it takes into account the different intensity of the public authority's interference in the subject's private life[412], but this order of things also shows

411 It is also the object of the vast majority of the requests.

412 During the discussion on the Proposal, the EESC has pointed out that also subscriber and access data are personal information: therefore, a judge should be involved in issuing the order as well: *Opinion of the European Economic and Social Committee*, n. 11533/18, July 12, 2018, *eur-lex.europa.eu*, point 1.7. The opinion, however, does not square with the fact that the prosecutor normally has access to personal data of the defendant or a person of interest in an investigation, without the judge being necessarily involved. Moreover, these types of data do not necessarily involve a third party, which can also justify a more relaxed standard.

one main critical aspect. Setting a threshold at three years of maximum custodial sentence is hardly a limit at all: in the Italian legal system, there is basically no petty crime that would not allow law enforcement authorities to ask for the disclosure of the most sensitive information on the scale[413]. To be fair, it is very hard to set a reasonable scope with this kind of legal instrument: regulations work immediately throughout the entire Union, regardless of how the criminal codes punish crimes within one state's borders. There is no harmonized criminal code; the harshness of punishment is for the single nation to decide and the European Union has little to do with that. However, three years of maximum custodial sentence seems to be too generous, and the proposal itself tries to justify the choice, aimed at not undermining «the effectiveness of the instrument and its use by practitioners»[414]. Yet, this explanation does not seem to be fully satisfactory. If effectiveness had to be a concern in this phase, it would have been better served by setting no general limit. On the contrary: effectiveness should be properly balanced with the proportionality of state's action, or the outcome could be an odd, efficient tool that systematically harms more individual rights than it is necessary and reasonable to do.

Now, let's have a closer look at the procedure. The issuing authority – a court, a judge, a prosecutor – can resort to those Orders during the investigation or the trial and has to comply with a series of instruction provided by the draft regulation. The document shall specify the issuing and (if necessary) the validating authority; the provider that the measure addresses; the person whose data are to be disclosed; the requested data categories; the criminal statute whose alleged violation is being investigated; a couple of other technical details and, most importantly, the ground for the necessity and proportionality of the measure[415].

This last requirement is particularly relevant when the issuing authority is asking for the disclosure of content and transactional information: in this case, a judge or a court shall validate the order, which would be a hard thing to do without a reasoned explanation on why this measure has to be taken and why it is proportionate.

In all other cases (production order for less sensitive data; preservation order) the prosecutor can do everything on his own; nonetheless, the grounds on which the action is taken should be specified: the person whose data have been sought could later challenge the legality of the Order, especially on those grounds. In the first part of the procedure, however, these explanations will remain between the issuing authority and itself.

The Proposal also states that an Order can be issued if a similar action is allowed under the issuing state's law, which is a difficult condition to verify: one of the points of departure for this drafted regulation is exactly the absence of national provisions on direct cooperation with service providers, and it is not clear how to establish an analogy. If the order demands the disclosure of stored communication, the closest proxy could be the national 'interception of communications,' that is only allowed under different standards. It is as if the regulation would like to impose uniform standards across the countries, but also wanted these two Orders to blend in the national system: it seems hard to have it both ways. At the end of the day, it is plausible for this clause to be disregarded: the Proposal sets its own limits, which are way easier to control and verify.

413 See also Meijer Commitee, 'CM1809 Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters', *statewatch.org*, 18 July 2018, p. 1.
414 *Proposal*, p. 16.
415 The complete list of requirements is contained by articles 5 and 6 of the Proposal.

Another circumstance that should prevent the adoption of a Production Order is the fact that the disclosure of those data would harm fundamental interests of the addressee's state, such as its national security and defense; or that the information would be privileged under the addressee's state law. The first condition deals with the protection of the other county's most delicate balance, and it is bizarre that such an evaluation is left to a single judicial authority of a foreign country. Probably it will have no means to assess the impact that such a request should have on another State's national security, and it is why those requests were managed through MLA to begin with. This trait has also been noticed by a member state that, during the discussion of the proposal, has underlined that it is important to involve also the addressee's state in the early stage of the procedure, to avoid an erosion of the state's sovereignty[416]. The same goes for the second possible issue: the assessment is not as difficult, but the single authority is supposed to know the precise extent of another country's laws establishing privilege, which does not seem realistic. Moreover, if the Italian law authority asked Facebook for the content data – including the messaging history – of the person A, it could stumble upon privileged communications that they did not expect to find there in the first place. It is not possible to know in advance the full extent of what does a service provider have, and it could be complicated to establish in advance whether the information is protected by the other state's law.

Let us assume that the Order has been issued. It is not still enough to address the company: the issuing authority needs to complete a Certificate[417] that can be sent directly to the provider, without any communication with the state where the provider is established. The certificate contains all the information that the Order had to provide, except for the necessity and proportionality justification: that content shall remain confidential, not to put the investigation at risk.

The addressee has then 10 days upon the receipt to send the relevant data to the issuing authority; it the EPOC is incomplete or contains error, the company has 5 days to ask for clarifications through the form provided for by the Annex III of the proposal.

The provider informs the user of the disclosure, unless it is not asked to keep the request confidential; in this case, the issuing authority will have to inform the person without delay about the execution of an EPOC (but not of an EPOC-PR), or they can postpone such a notification until when it would not damage the investigation. According to the proposal, this provision has been shaped following the example of the EIO directive: its art. 19 provides for precautions to preserve confidentiality. This parallel, however, does not seem to hold too well: art. 19 of the Directive is addressed to a judicial authority of another member state, and not a private company. Only the last paragraph mentions banks, but it points out that the States should take the necessary measures to prevent them from disclosing their cooperation with an ongoing investigation. The approach seems radically different here: the general rule is that providers – a private corporation – can give notice to their clients unless they are explicitly prohibited to.

Assuming that the addressee is (or was) providing a service to the suspect and that the EPOC appears to be legitimate and complete, there is still a window of legitimate non-compliance

416 See the Note from the General Secretariat of the Council to the Delegations, Interinstitutional File n. 2018/0108(COD), June 26, 2018 (hereafter: Note), *eur-lex.europa.eu*, p. 6.

417 The Proposal also provides for the templates: the European Production Order Certificate (EPOC) template is referred to as Annex I; the European Preservation Order Certificate (EPOC-PR) as Annex II.

with the request, and the drafted regulation does envisage two main kinds of reasons for that: technical and legal.

As for the technical side, the data could have been canceled due to the ordinary data retention obligations, or upon request of the user. Those are listed under the 'de facto impossibility', that gives the provider a legitimate reason not to answer[418]. It could also avoid liability if it is not answering because of force majeure.

As for the legal reasons, the provider could take issue at the manifestly abusive EPOC or at the request that violates the Charter of Fundamental Rights of the European Union. If this is the case, the addressee can reject the EPOC and send a copy of the rejection form to its EU home-state, so that the competent authorities can ask for clarifications to the issuing authority.

Moreover, the EPOC could conflict with a third country's legislation on data disclosure, and at that point, the addressee would be put in a "damn you if you do, damn you if you don't" kind of situation. The conflict of obligation has to be notified to the issuing authority and argued in depth by the provider, that also must point out the rules that are relevant to the case and how they contradict the European obligation.

Both the evaluations require a deep knowledge of the law and the necessary skills to apply it, and they are quite extraordinary tasks to be assigned to the legal department of a private corporation. Besides, not all service providers are trillion-dollar-worth conglomerates with the necessary resources to hire the sharpest legal minds on the market: some of them are middle-sized companies and playing the judge would be quite demanding[419].

In case of non-compliance, however, the issuing authority can decide to ask the relevant member state to execute the measure: first, the Order has to be recognized. This approval should be given without formalities and would bring to a second round of cooperation with the original addressee, that can oppose the order again, for the same set of reasons. At that point, the executing state can impose sanctions.

The picture appears to be quite convoluted: the procedure is basically put in place since its inception, but carried out by the competent member state, which should act upon the Order written by a foreign authority. This step of the procedure is the only one to be directly linked to the principle of the mutual recognition (art. 82 TFEU), and yet it pointed to as the legal basis for the entire regulation.

5. The compact territoriality of the national state clashes with the diffused territoriality of the cloud and they are not easy to reconcile. Sure, unilateral action is a captivating method: it promises quick results, but it also unbalances the system. The providers are charged with a role for which that

418 To a certain extent, the *de facto* possibility depends on the policy of the provider: after the San Bernardino case, for instance, many messaging applications shifted to end-to-end encryption (before – among the mainstream apps – it was implemented by the secret conversations of Telegram): the message is stored in a server, but the company cannot open it; only the users (the two ends of that communication) have the key. For more on the topic, see: R. Budish, H. Burkert, U. Gasser, *Encryption Policy and Its International Impacts*.

419 Those expectations have already been defined as "unrealistic": see Note, p. 6-7. For another critical view on the point, see V. Mitsilegas, *The privatization of mutual trust in Europe's area of criminal justice. The case of e-evidence*, in *MJECL*, August 9, 2018.

they have no authority (or credibility)[420], the states go searching for information at the risk of harming even national security of another country.

This approach, however, does not seem consistent with the role of sovereignty as we know it. To implement a coherent solution, we should reconceptualize the concept to make it compatible with a liquid cloud. Besides, the other path forward is to give MLA a serious try, by investing in bilateral or multilateral treaties which could provide for easy and standardized procedures, secure portals for the presentation of the requests and a user-friendly system to check and answer them.

LAURA BARTOLI

420 It is just a step forward in a known direction; service providers have already been charged with institutional tasks: see E. Haber, *Privatisation of the Judiciary*, in Seattle University Law Rev., 2016, 115.

II.4

Towards an alternative to territorial jurisdiction to face criminality committed through or facilitated by the use of blockchains

SUMMARY: 1. Introduction. – 2. The territoriality principle to determine State jurisdiction. – 3. The development of cybercrime and its consequences on the territoriality principle. – 4. The development of blockchains and its consequences on the territoriality principle. – 5. The applicability of the targeted public theory to establish jurisdiction over offences enabled or facilitated by the use of blockchains. – 6. Towards an alternative to State jurisdiction based on territoriality. – 7. Conclusions.

1. According to Christopher Pierson, « States occupy an increasingly clearly defined physical space over which they claim sole legitimate authority[421]». The territoriality principle supposes that a State has authority to exercise jurisdiction over conducts taking place within its own territory[422]. At the birth of the modern State, the territoriality principle was subject to almost no doubt or question. However, the globalisation of the world, especially through the development of technological means and through the Internet, marked a real change of society and raised new legal questions. In a society which is built globally, jurisdiction based on national borders does not make sense anymore. According to Darrel C. Menthe « [...] cyberspace takes all of the traditional principles of conflicts-of-law and reduces them to absurdity[423] ». After the launch of Bitcoins, ten years after this quotation, Darrel C. Menthe could have said the exact same thing about blockchains[424].

The objective of this article will be to assess whether the territoriality principle in its current form may be used in order to tackle offences facilitated by or committed through a blockchain. The developments to the territoriality principle resulting from the raise of cybercrime will be used as a background. Finally, some of the proposals that have been made by scholars will be assessed in order to imagine an alternative to State jurisdiction based on territoriality to overtake criminality committed through or facilitated by the use of blockchains.

In order to do this, the concept of territoriality as it is used in order to determine State jurisdiction over an offence will be studied (2), then the consequences of the development of the Internet and cybercrime on State jurisdiction established through the territoriality principle will be assessed (3). The fourth part of this article will study the development of blockchains and its

421 C. PIERSON, *The modern State*, London, 2002, II ed., p. 9, http://psi424.cankaya.edu.tr/uploads/files/Pierson,%20The%20Modern%20State,%202nd%20ed.PDF.

422 D. IRELAND-PIPER, *Extraterritorial criminal jurisdiction: Does the long arm of the law undermine the rule of law*, in *MJIL*, 2012, p. 130.

423 D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, in *MTLR*, 1998, p. 71.

424 For more clarity, within this article, Blockchain should be understood as a transparent, secure information storage and transmission technology that operates without a central control body (the "Blockchain"). By extension, a blockchain is a database that contains the history of all exchanges between its users since its creation. This database is secure and distributed: it is shared by its various users, without intermediaries, which allows everyone to check the validity of the chain.

(a "**blockchain**") – definition provided by Blockchain France, https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/.

consequences on the territoriality principle (4) before studying the applicability of the targeted public theory to establish jurisdiction over offences enabled or facilitated by the use of blockchains (5) and finally, it will move on to review some of the proposals made in order to better respond to cybercrime and analyse their applicability to criminality enabled or facilitated by the use of blockchains (6).

2. Sovereignty constitutes one of the founding principles of the modern State. The Peace of Westphalia, which constitutes for scholars the beginning of the modern international system, implied the concept of Westphalian sovereignty. This concept supposes the inviolability of borders, the equality between all sovereign States and above all, the non-interference in the affairs of foreign States[425]. The principle of national sovereignty supposes that « within the limits of its jurisdiction (set by the division of the world into a series of similarly sovereign nation-states), no other actor may gainsay the will of the sovereign State[426] ». This Westphalian sovereignty principle is stated in article 2(4) of the United Charter, according to which « Members thus, shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations ». No limitation to the power of the State can be brought by another. The right to punish (*ius puniendi*) expresses the Sovereign's authority throughout its population and territory. This means that only the State should have a right to punish individuals on its own territory[427]. Therefore, criminal law constitutes the core of the State's Sovereignty[428]. The principle of territoriality in criminal law confirms the sole authority and jurisdiction of the States and the right to punish it has on its citizen and within its territory.

The territoriality principle – to be understood as the right for a sovereign State to prosecute offences committed within its territory – is recognised by public international law. Public international law makes a distinction between subjective and objective territoriality[429]. Subjective territoriality should be understood as the right to prosecute offences committed – or at least initiated – within the territory of the State when objective territoriality gives the right to prosecute offences initiated within the territory of another State but that are completed[430] or whose effects are to be felt

425 B. TESCHKE, *La théorisation du système étatique westphalien: les relations internationales de l'absolutisme au capitalisme*, in *CRS*, 2012, p. 31; W. BERGE, *Criminal jurisdiction and the territorial principl*e, in *MLR*, 1931, p. 240; S. GARIBIAN, *Souveraineté et légalité en droit pénal international: le concept de crime contre l'humanité dans le discours des juges à Nuremberg*, in M. HENZELIN, R. ROTH (eds.), *Le droit pénal à l'épreuve de l'internationalisation,* Paris-Genève-Bruxelles, 2002, p. 2, https://archive-ouverte.unige.ch/unige:23564.

426 C. PIERSON, *The modern State*, cit., p. 11.

427 S. GARIBIAN, *Souveraineté et légalité en droit pénal international: le concept de crime contre l'humanité dans le discours des juges à Nuremberg*, in M. HENZELIN, R. ROTH (eds.), cit., p. 2.

428 On the role of criminal law as the core of the State's sovereignty, see for example B. MATHIEU, M. VERPEAUX, *Droit constitutionnel*, Paris, 2004, paragraph 384.

429 J. B. MAILLART, *The limits of subjective territorial jurisdiction in the context of cybercrime*, in *ERA Forum*, 2018, p. 3, https://link.springer.com/article/10.1007/s12027-018-0527-2#Fn7.

430 The objective territoriality has been recognised at an international level in the Lotus Case, Permanent Court of International Justice, *S.S. Lotus (Fr. v. Turk.)*, 7 September 1927, series A, no. 10, https://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf.

within the territory of the State[431]. This extensive comprehension of the territorial principle follows the ubiquity theory, which recognises the possibility for an offence to be present in more than one place. The ubiquity theory supposes that an offence may be located where any of its constituent element are located – this may be the place where the offence itself took place but also the place where the effects of the offence took place[432].

We find similar rules of jurisdiction at the national levels. Therefore, it does make more sense to refer to the objective and passive territoriality as they result from international law than to refer to specific national jurisdiction rules that would echo these principles. For example, French criminal law is applicable to offences committed within the territory of the Republic[433]. However, since it is not that easy in practice and since offences are often committed only partly in a certain State, the notion of offence committed within the territory is viewed in an extensive way. Thus, the concept includes all of the offences whose only one of the constituent elements took place in France[434]. German criminal law is also applicable to all offences that were committed in Germany[435]. An offence is to be understood as committed on the German territory either when the agent acted or when the effects of the offence are to be felt in Germany[436]. Additionally, an offence is considered as committed within the territory of Italy when the constituent element to the offence happened entirely or in part in Italy or if the consequence of the constituent element to the offence happened in Italy[437].

The globalisation of the world that we perceive tends to enable the development of social relations beyond territorial constraints. Because of the global character of the social relations of our era, of course, such a conception of territoriality accepts the risk that different jurisdictions may be established over a same offence, whose constituent elements are located in different countries that may all have jurisdiction over the conduct[438]. It is sometimes argued that, even though the Internet was first referred as a lawless area[439], the ubiquity theory finally renders it an overflow of repressive powers[440].

431 C. RYNGAERT, *The concept of jurisdiction in international law*, Oxford, 2015, II ed., p. 5, https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf; D. IRELAND-PIPER, *Extraterritorial criminal jurisdiction: Does the long arm of the law undermine the rule of law*, cit., p. 130.

432 H. ASCENSIO, L'*extraterritorialité comme instrument*, in *Travaux du Représentant spécial du Secrétaire général des Nations Unies sur les droits de l'homme et entreprises transnationales et autres entreprises*, 2010, p. 5, https://www.rse-et-ped.info/IMG/pdf/10-12-10_Ascencio_extraterritorialite-1.pdf.

433 French penal code (*Code pénal*), article 113-2-1 and French code of criminal procedure (Code de procédure pénale), article 693.

434 French penal code (*Code pénal*), article 113-2-2.

435 German penal code (*Strafgesetzbuch*), section 3.

436 German penal code (*Strafgesetzbuch*), section 9 paragraph 1.

437 Italian penal code (*Codice penale*), article 6.

438 L. DESESSARD, *France, les compétences criminelles concurrentes nationales et internationales et le principe ne bis in idem*, in *RIDA*, 2002, p. 917.

439 T. SCASSA, R. J. CURRIE, *New first principles – assessing the Internet's challenges to jurisdiction*, in *Geo. J. Int'l L.*, 2011, p. 1037; A. C. YEN, *Western Frontier or Feudal Society?: Metaphors and perceptions of cyberspace*, in *Berkeley Tech. L.J.*, 2002, p. 1037.

440 R. BOOS, *La lutte contre la cybercriminalité au regard de l'action des État,* 2016, p. 162, https://tel.archives-ouvertes.fr/tel-01470150/document.

3. While the Council of Europe Convention on cybercrime (the "Convention")[441] does provide for examples of what should be considered a cybercrime and thus, should be tackled by national substantive criminal law, the Convention does not provide for a general definition of cybercrime. However, the doctrine seems to agree on a rather large definition of cybercrime: Majid Yar defines cybercrime as any illegal activities facilitated by a computer[442] while Sarah Gordon and Richard Ford define it as any crime committed through or facilitated by the use of electronic devices or IT networks[443]. Thus, any offence enabled or facilitated by the use of a blockchain may also fall under this definition and it should therefore make sense to use the legislation on cybercrime as a background in order to try to apply it to criminality committed through or facilitated by a blockchain.

Throughout the last decades, we observed a global integration of the world which enhanced the interactions among people at a global level. This enhanced integration at a global level has been the consequence of, amongst others, the development of technology and of the Internet. The development of the Internet has been accompanied by the one of criminality facilitated by the use of the Internet and the law had therefore needed to respond to such a phenomenon. However, the particularity of cybercrimes raised certain difficulties that the territoriality of criminal law has to face. We should recall that the Internet is a network; the communications it contains are not limited to a specific territory. « Material published on the internet can be uploaded in one state, downloaded in another, and viewed in a large number of other states[444] ». What raises some difficulties is the fact that the jurisdiction is based on delimited territorial rules while the Internet is, on the contrary, characterised by its universality[445]. Conducts on the Internet happen at once anywhere and nowhere: it seems thus difficult to decide which jurisdiction is more entitled to have jurisdiction over an offence than another one[446]. « Unlike traditional jurisdictional problems that might involve two, three, or more conflicting jurisdictions, the set of laws which could apply to a simple homespun webpage is all of them[447] ». For an offence committed online, any State may be competent[448]. This can be explained by the fact that, through the use of the Internet, an illegal content may be made available by an agent in a foreign country, through the use of a foreign server for data storage, but

441 Council of Europe, *Convention on cybercrime*, Budapest, 2001, ETS 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

442 M. YAR, *Cybercrime And Society*, 2006, London, p. 10.

443 S. GORDON, R. FORD, *On The Definition And Classification Of Cybercrime*, in *J. Comput. Virol.*, 2006, p. 2, https://download.adamas.ai/dlbase/ebooks/VX_related/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf.

444 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, in *JTLP*, 2013, p. 1, https://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/124/127.

445 J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, 2014, http://www.penal.org/sites/default/files/files/RH-7.pdf.

446 S. P. BEATTY, *Litigation in cyberspace: the current and future state of Internet jurisdiction*, in *U. Balt. Intell. Prop. L.J.*, 1999, p. 139; D. R. JOHNSON, D. POST, *Law and borders – the rise of law in cyberspace*, in *Stanford L. Rev.*, 996, p. 1375.

447 D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, cit., p. 71.

448 D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, cit., p. 70.

still making the illegal content available to any person benefiting of an Internet access in any State[449]. Therefore, we understand that the principles that we developed in the first part of the article, that are used to establish jurisdiction, may be difficult to apply to the cyberspace.

Regarding the subjective territoriality: first, we understand that, because of the global character of the Internet and the multiplicity of its actors, it may be difficult to determine where an offence took place. The complexity related to the localisation of the causal event has been highlighted by the Advocate General Wathelet in the case Concurrence SARL v. Samsung Electronics France SAS and Amazon Service Europe Sàrl[450]. In order to respond to this, it should be determined in which territory is located an offence on the Internet? There are many possibilities to decide what constitutes the location of the offence: the location of the author or creator of the illegal content may be one but it would however face the risk of forum shopping to choose the most clement jurisdiction to commit an offence. We could also quote some others such as the location of the viewer of the illegal content, but it would not prevent positive conflicts of jurisdiction[451]. Therefore, regarding cybercrime, Lord Denning said that « a well-advised plaintiff is likely to commence proceedings in the most favourable forum[452] ». This is particularly relevant since a similar conduct on the Internet may be tackled in a complete different manner according to the competent jurisdiction. The location of the server giving access to the Internet and enabling the upload of illegal content may also be a solution. The location of the server may be difficult to determine because of technical issues and because of the possible use of multiple sub-servers. We could finally think about the first location of the website containing the illegal content to establish jurisdiction[453]. So far, we have no consensus on what constitutes the place of location of an offence on the Internet, this is why positive conflicts of jurisdiction may therefore not be solved by the use of subjective territoriality.

Regarding the objective territoriality: since the Internet is available almost everywhere, the constituent elements to a crime occurring on such an Internet page, may be located anywhere; in fact, in any jurisdiction that provides for access to the website. If this was the case, the territorial principle would not make sense anymore since by using it, it would give jurisdiction to any State. Therefore, the competence would tend to be a universal one[454]. Finally, the consequence would be

449 M. D. DUBBER, T. HÖRNLE, *Criminal law a comparative approach*, Oxford, p. 149.
450 Advocate General WATHELET, 9 November 2016, *Opinion on Concurrence SARL v Samsung Electronics France SAS and Amazon Service Europe Sàrl*, Case C-618/15, ECLI: EU:C:2016:843, paragraph 2.
451 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2; H. VAN LITH, *International jurisdiction and commercial litigation: uniform rules for contract disputes*, The Hague, 2009, p. 5 ss. Also see a similar theory for copyrights law on the internet in T. SOLLEY, *The problem and the solution: using the Internet to resolve Internet copyright disputes*, in *Ga. St. U. L. Rev.*, 2008, p. 818.
452 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2; *Forum Shopping reconsidered*, in *Harvard L. R.*, 1990, https://www.jstor.org/stable/pdf/1341283.pdf.
453 For more information on the pro and contra arguments related to these different possibilities, see S. F. MILLER, Bloomingtom, 2003, p. 235 ss, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1270&context=ijgls.
454 J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, cit.

constant positive conflicts of jurisdiction[455]. So, using the objective territoriality does not solve the problem of positive conflicts of jurisdiction[456].

If the traditional rules of jurisdiction are used without taking into account the specificity of the Internet, this would lead not only to incoherencies but also to a lack of legal certainty[457]. While criminal law should respect the principle of legality which supposes that it should be not only clear but also predictable[458] and that « punishment, coercive measures, prosecution and sentencing of criminals should be predictable and be applied uniformly and in a systematic order[459] » these uncertainties constitute a problem if they lead to as many different solutions as the number of potential competent States (which, as we have seen before, is extremely high). The fact of being potentially subject to all of the criminal law systems of the world may constitute a threat vis-à-vis of fundamental principles of criminal law – especially vis-à-vis the legality principle. This could also endanger the principle of *ne bis in idem* if more than one jurisdiction is competent and decide to prosecute the same offence committed online. As a consequence, legal certainty – which encompasses both the legality and the *ne bid in idem* principles[460] – may be weakened by the inadequacy of traditional jurisdiction rules to face cybercrime and this may endanger the rule of law in the information society, which reposes on principles including, amongst others, the certainty and predictability of the legal environment[461].

In 2001, the Council of Europe published a Convention on cybercrime. In its explanatory report regarding the Convention, the Council of Europe explained that it was aware of the necessity to use international law in order to address such a form of criminality that produces effects regardless of borders and regardless of the location of the offender[462]. The challenge that constituted the global character of the Internet was taken into account by the Council of Europe, which distinguished the creation of a common space – the cyberspace – which may be used to commit offences at a transnational level[463]. In its explanatory report, the Council of Europe recognised the fact that criminals using the Internet may be located in places different to those where the offences they commit produce their effects[464]. This was notably the reason why the Council of Europe argued

455 M. DELMAS-MARTY, *Le relatif et l'universel. Les forces imaginantes du droit*, tome 1, Paris, 2004, p. 342.
456 J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, cit.; K. N. EDWIN, J. SHILILU, *Jurisdictional challenge of the Internet ; a focus on electronic contracts*, p. 3, http://www.academia.edu/27265774/JURISDICTIONAL_CHALLENGE_OF_THE_INTERNET_A_FOCUS_ON_ELECTRONIC_CONTRACTS.
457 Z. D. CLOPTON, *Territoriality, technology, and national security*, in *U. Chi. L. Rev.*, 2016, p. 49.
458 On the exigence of quality of the law according to the European convention on human rights, see for example, European Court of Human Rights, *Cantoni c. France*, no. 17862/91, 15 November 1996.
459 A. SUOMINEN, *What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?*, in *BJCLCJ*, 2014, p. 7.
460 A. SUOMINEN, What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?, cit., p. 9.
461 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2.
462 Council of Europe, *Explanatory report to the Convention on cybercrime*, ETS 185, Budapest, 2001, paragraph 6, https://rm.coe.int/16800cce5b.
463 Council of Europe, *Explanatory report to the Convention on cybercrime,* cit., paragraph 8.
464 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 6.

for the necessity to tackle the challenge of cybercrime at an international level[465]. Therefore, the Council of Europe decided to tackle the question of jurisdiction and more precisely the issues regarding the determination of the place of commission of the offence[466]. However, even if the Convention provides for State parties to exercise jurisdiction when an offence is committed on their territory, it does not give specific rules on what should be considered an offence committed in a State's territory. The only way provided for by the Convention in order to deal with positive conflicts of jurisdiction is that it provides for States to consult to determine among them which State constitutes the most appropriate jurisdiction for prosecution, when more than one State has jurisdiction over an offence according to the jurisdiction rules provided for by the Convention[467]. This should be done in order to « avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings[468] ». It is a big step to focus on the regional level in order to find solutions to a global problem instead of focusing on national rules. However, the Convention and the rules it provides on jurisdiction, even if they can help because of the cooperation that they provide for, do not really give clear rules on territoriality that would permit to prevent positive conflicts of jurisdiction.

At a national level, judges confronted to jurisdiction issues within cybercrime cases, often relied on the objective territoriality principle. In the Töben case, the German court held that jurisdiction of German courts may be established solely because Internet users located in Germany could have access to the content that constituted a criminal offence, even if this content had been created and stored in foreign States. The Court considered that the offence had consequences (if not only, at least also) in Germany and the objective territoriality principle should thus give jurisdiction to Germany. Before 2008, the French jurisprudence also considered that the French jurisdictions were competent as soon as illicit content were available on the Internet and were accessible from France: thus, as soon as the website containing the criminal offence was accessible from France, jurisdiction was established[469]. This view was taken in the Yahoo! case in which the French jurisdictions declared themselves competent to hear the case because the website was available in France, even if it was not supposed to be intended for the French public[470]. However, conscious of the risks that the application of the objective territoriality principle means in terms of positive conflicts of jurisdiction, a French court in 2008[471] took a different view regarding cybercrimes. The French jurisdiction decided that it is not sufficient that the content on the website which constitutes

465 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 6.
466 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 11(v).
467 Council of Europe, *Convention on cybercrime*, Budapest, 2001, ETS 185, art 22(5), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.
468 Council of Europe, *Explanatory report to the Convention on cybercrime*, cit., paragraph 239.
469 Groupe de travail CECyF – Cyberlex, *La procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique : propositions pour une efficacité juridique renforcée*, 24 janvier 2018, p. 6 ; Tribunal de grande instance de Paris, CCE 2002/5. Comm. 77, 26 February 2002.
470 A. CAMARD, C*ommentaire des arrêts Yahoo v. La ligue contre le Racisme*, in *MBDE/Société de l'information, droits et médias*, 2011.
471 Cour de Cassation, chambre criminelle, no. 07-87.281, 9 September 2008, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000019570259&fastReqId=850465415&fastPos=1.

the criminal offence is accessible on the French territory, but it should also be proved that the website in question is dedicated to the French public. Certain advices may help in order to decide whether a website is dedicated to the French public: these include, for instance, the language of the website or also the fact that the products sold on the website are available to French citizens[472]. This view was confirmed by the French Court of cassation in 2010[473]. This trend can also be distinguished in other national laws[474]. Especially, the United States introduced such jurisdiction rules based on the targeting of a specific public by making a distinction between active and passive websites[475]. A passive website should be considered insufficient to establish jurisdiction when an active website may give jurisdiction to the State's courts. The principal criteria to be taken into account in order to determine whether a website is to be considered as active in a State is: the fact that the website is interactive, that it conducts business in the State and that it is advertised to potential customers in that State.[476]

4. What we distinguished with the development of the Internet was a simultaneous development of criminality facilitated by it. Even though this phenomenon had to be tackled by law enforcement authorities, this did not become a reason to over regulate the Internet or to diabolise it. The same approach should be taken with regard to blockchains. While certain authors consider blockchains and cryptocurrencies as too risky and plead for very strict rules[477] and while some countries decided to completely ban the use of cryptocurrencies[478] because of the possible threats it contains, many scholars stress the fact that these potential risks should in no way be used in order to reject the advancements in technology and innovation[479]. A distinction should always be made between the positive and the negative effects of the technology and the existence of negative effects should not have consequences that would detriment the positive ones. However, this should not be a reason to ignore the criminal activities taking place within the Blockchain ecosystem. The objective of the article is not to highlight the phenomenon of criminality committed through or facilitated by the use of blockchains or cryptocurrencies, but just to raise awareness regarding its existence: Interpol identified amongst others, the use of blockchains for sharing illegal data such as child pornography while Europol highlighted the risk of money laundering facilitated by the use of cryptocurrencies[480]. There are two different ways blockchains may be used for criminal purposes:

472 See for example, Cour de Cassation, chambre criminelle, no. 15-86645, 12 July 2016, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000032900131.
473 Cour de Cassation, chambre criminelle, no. 10-80.088, 14 December 2010, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000023433809.
474 T. SCASSA, R. J. CURRIE, *New first principles – assessing the Internet's challenges to jurisdiction*, cit., p. 1049.
475 R. BOOS, *La lutte contre la cybercriminalité au regard de l'action des État,* cit., p. 175 ss.
476 See for example *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, W.D. Pa, 1997, https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/; *Cybersell Inc v. Cybersell Inc.*, 130 F.3d 414, 9th Cir., 1997, https://www.courtlistener.com/opinion/748638/cybersell-inc-v-cybersell-inc/.
477 See for example E. ENGLE, I*s Bitcoin rat poison? Cryptocurrency, crime and counterfeiting*, in *JHTL*, 2016.
478 M. DI GIUDA, *Countries where the cryptocurrencies are banned: busted for Bitcoin*, 2018, https://bitnewstoday.com/market/bitcoin/countries-where-the-cryptocurrencies-are-banned-busted-for-bitcoin/.
479 R. ANDERSON, *Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age*, in *Consumer Payment Innovation*, 2012, p. 99.
480 *Report of the Commonwealth Working Group on virtual currencies*, in *Commonwealth Law Bulletin*, 2016, p. 292.

either as instrumentality of the crime – in this case the offence would just be facilitated by the use of blockchain but could have been conducted in other ways also (one could for instance think about money laundering or the selling or buying of illicit products with cryptocurrencies) or the blockchain may be the object of the crime which could not have been committed without the existence of blockchains[481]. For example, one could think about the theft of cryptocurrency or broadcast of child pornography pictures through blockchains.

Thus, criminality committed through or facilitated by the use of blockchains – and especially the jurisdiction dilemma – constitutes an issue for the criminal justice systems that they should be able to tackle.

In the third section of this article, when trying to deduce what may constitute the place of location of an offence committed on the cyberspace, we highlighted the multiplicity of the actors within the Internet ecosystem. Especially, we developed the possibility to focus on the location of the viewer of the illegal content, the location of the creator of the illegal content, the one of the server enabling the publication of the content and finally the first location of the website in order to establish jurisdiction. We distinguish a similar – if not worse – multiplicity and transnationality of the actors on a blockchain. The first actor to mention is the creator(s) of the blockchain. Then, we should mention the different users of the blockchain – also called nodes. The system has been designed as an open one: this means that it is, by its very nature, open to anyone (in the case of a public blockchain) and thus also internationally open since any individual who wishes to participate to the public blockchain may be given a pair of keys randomly by the system. The existence of miners should also be highlighted. Miners should be understood as special nodes whose role is to verify the transactions by performing a proof-of-work or any similar consensus mechanism in order to accept the valid transactions in a block that will then be added to the blockchain. Finally, even though the functioning of a blockchain only requires the participation of nodes and miners, some other actors exist around the ecosystem. They render its use easier for non-technicians and as a consequence, more accessible. The ones mentioned in this paragraph do not constitute an exhaustive list of the actors existing around the Blockchain ecosystem: the purpose is only to focus on some of them, which are commonly used by participants. One could think about exchange platforms (whose activities consist in providing people with exchange services between fiat currency and cryptocurrency for example) and we could also mention digital wallets (whose activities consist in storing the users' information on the blockchain including their public and private keys).

Blockchains are also known as distributed ledgers. This supposes that the data within the blockchain is distributed to all of the nodes of the system instead of being concentrated into one as it is the case for centralised ledgers. Therefore, all of the participants to the network gets a copy of the blockchain as it currently is. Each block that is added to the blockchain is also added at the nodes' level so that there is a consensus between the nodes on the state of the register[482]. Distributed ledgers require the consensus of these nodes rather than just the confirmation by one central authority in order to add information on the blockchain. This means that, even though a miner

481 *Report of the Commonwealth Working Group on virtual currencies*, in *Commonwealth Law Bulletin*, cit., p. 292.
482 G. MARIN-DAGANNAUD, *Le fonctionnement de la blockchain*, in A*nnales des mines: réalités industrielles*, 2017, p. 43.

validates a block, it still needs to be accepted and reused by the other nodes of the system to be integrated to the blockchain: a consensus of a majority of the nodes is needed. « Each resulting block is forwarded to all users in the network, who can then check its correctness by verifying the hash computation. If the block is deemed to be "valid", then the users append it to their previously accepted blocks, thus growing the [...] blockchain[483] ». Because of this consensus mechanism, we distinguish a joint control of the blockchain.

According to international law, the competent jurisdiction is usually either the State where the offence has been initiated (subjective territoriality) or the State where the offence is completed or its effects are to be seen (objective territoriality and ubiquity theory); in the specific case of a criminal conduct taking place on a blockchain, these States may be difficult to identify. This can be explained by the fact that the activities taking place on blockchains operate themselves without any particular spatial linkage since blockchains are developed in a global way and the localisation of the actors does not have a strong importance[484].

Regarding the subjective territoriality, it may be difficult to determine the State where the offence has been committed and what the competent jurisdiction should be. The multiplicity and global character of the actors to the blockchain – either essential or not to the functioning of the system – and also, the fact that the conducting of a transaction result from the actions of many different actors – possibly located in different jurisdictions – complicates the determination of the place of commission of the offence. It may be difficult to decide on which territory such an offence has been committed if we try to distinguish a single jurisdiction that could tackle the offence. On the contrary, we could argue that many countries may have jurisdiction over such an offence if not all of them – because of the multiplicity and internationality of the different nodes to the blockchain[485]. The subjective territoriality aims at finding some links and thus a jurisdiction that would have more legitimacy to be declared competent. As we realise the global character to a transaction happening on a blockchain, it may be questioned whether there is such a State that would have more legitimacy than another one to conduct investigations.[486]

Regarding the objective territoriality, it may also be difficult to determine where an offence committed through or facilitated by the use of blockchains is completed or where it has effects. As a blockchain is distributed to all of its nodes, the effects may be felt in any jurisdiction which gives access to the blockchain and permits individuals to join the network. As a consequence, if the Internet was seen (rightly) as a transnational technology that enabled to make content available in any State simultaneously, distributed ledgers share also this transnational characteristic but in a

483 A. MALLARD, C. MÉADEL, F. MUSIANI, *The paradoxes of distributed trust: peer-to-peer architecture and user confidence in bitcoin*, in *Journal of peer production*, 2014, p. 6, https://hal-mines-paristech.archives-ouvertes.fr/hal-00985707/document.

484 For a similar reasoning regarding the financial economy, see J. B. AUBY, *La globalisation, le droit et l'Etat,* IIe ed., Paris, 2010, p. 20.

485 On top of the fact that determining the location of an offence on a blockchain may be difficult because of the multiplicity of its nodes and the fact that they all contribute to the functioning of the system, this distribution of the blockchain and the consensus mechanism raise additional issues regarding criminal responsibility. This comes from the fact that the addition of a block to the blockchain results from the acts of many different nodes and that, the behaviour of one only node is not sufficient to modify the blockchain.

486 Private blockchains may however raise different issues, notably because of the fact that certain activities, such as mining, may be limited to certain actors.

more developed way, because of the fact that they are (as their name supposes it) distributed and thus, that any node to the network is provided with an accurate version of the blockchain.[487]

5. Blockchains function without the intervention of any central authority or third party. The functioning of the system is ensured only through the participation of the nodes and through the work of the miners. Thus, the participants to the blockchain only need to have confidence in the system and its protocol: the participants do not need to trust themselves in order to transact or to make sure that the person they plan to transact with is trustworthy. Therefore, a third party or central authority, whose role would be to ensure that the participants are well-intentioned and that the transactions are feasible, is not needed. However, these characteristics correspond in reality to only a subgroup of the Blockchain ecosystem: public blockchains, also known as permissionless blockchains. On the contrary, private blockchains (also known as permissioned blockchains) do not share all of these characteristics. Their functioning in a technological way is similar to the one of public blockchains but there is a considerable difference: a kind of central authority does exist and exercises a certain control. The authority is in charge of deciding who should be given a right to participation to the blockchain. This means that these private blockchains are, contrary to public blockchains, not open to anyone but only to those who got provided with an access right to the system by the authority[488]. The development of private blockchains can be at least partly explained by the inadequacy of public blockchains to tackle the need of regulated activities (such as the activities of the financial sector).

A private blockchain, contrary to a public blockchain, often has a Constitution (or other similar documents) that should have some legal effects[489]. This document which may for instance be a whitepaper and Terms and Conditions in the case of ICOs - should contain classical elements to a contract, including the governing law and jurisdiction[490]. Of course, from a legal perspective, this Constitution or any similar document are private contracts. Criminal jurisdiction is not subject to the individuals' disposition and may therefore not be chosen by the parties to a contract. Thus, it would make no sense to introduce a clause that would provide for the competence of a specific jurisdiction that would be competent over an offence in such a document. However, these documents may provide for some advices regarding the targeted public of the private blockchain.

We should recall the French jurisprudence tackling cybercrime and which considers that to establish competence of the French jurisdictions, it is not sufficient to demonstrate that the website was available in France but it should also be demonstrated that the website was dedicated to the French public. The advices that could help to deduce to which public the website was targeting

487 Private blockchains may also raise different issues, notably because of the fact that reading the blockchain may be limited to certain actors.

488 P. WAELBROECK, *Les enjeux économiques de la blockchain*, in *Annales des Mines - Réalités industrielles,* 2017, p. 10.

489 A. SANITT, I. GRIGG, Norton rose Fulbright, *Legal analysis of the governed blockchain*, 2018, http://www.nortonrosefulbright.com/knowledge/publications/167968/legal-analysis-of-the-governed-blockchain.

490 For instance, the Booking Token Unit's whitepaper specifies that any contract relationship relating to the tokens' protocol are governed by French law, V. CHRIQUI, H. HABABOU, *Whitepaper Booking Token Unit (BTU) Protocol*, 2018, p. 21, https://www.btu-protocol.com/pdf/whitepaper.pdf, also, the Crypto20 Token terms and conditions provides for the applicability of English law as the governing law, Crypto20, Terms and conditions, https://crypto20.com/en/legal/.

include the language of the website or also its content. A similar reasoning could be made regarding private blockchains. Thus, we could argue that the Constitution of a private blockchain targets also a specific public (that may not be limited to a certain country but that may be limited to a certain number of States) such as the Whitepaper of an ICO by selling its tokens to a specific public and by describing the legal statute of blockchains in certain countries[491]. Also, the language of publication of the documents of the blockchain may be taken into consideration[492]. As a consequence, if we stick to the advices distinguished by the French jurisprudence that may be useful in order to deduce the targeted public of a specific website, a similar reasoning could be made with regards to private blockchain: the targeted public may be deduced from the documents to the blockchain and may help to establish jurisdiction.

This targeted public theory, even though it may be useful in the context of private blockchains may be insufficient to establish jurisdiction over offences committed through or facilitated by a public blockchain because these networks are, by nature, open to anyone. If we take the example of the Bitcoin blockchain, we can see that it is used worldwide and it is in no case targeting a special public located in a certain country. Therefore, we understand that the national rules permitting to establish criminal jurisdiction according to the territoriality principle may not be sufficient in order to tackle the phenomenon of criminality facilitated or committed through the use of blockchains or cryptocurrencies – as they were not sufficient to tackle the issue of cybercrime. While private blockchains may give some pieces of advice in order to decide which jurisdiction should be competent, public blockchains do not propose such tools. Thus, the same consequences that we highlighted from the uncertainties about jurisdiction rules regarding cybercrime can be made regarding blockchains: they may result in numerous positive conflicts of jurisdiction. This may weaken the principle of legal certainty and the principles of the rule of law.

6. According to Amartya Sen, the indispensable response to the doubts about globalisation resides in its construction[493]. This supposes that globalisation in terms of criminal matters and more specifically in our case, in terms of territoriality, should be built. In order to do so, it should be accepted that the territoriality of criminal law should be rethought because of its inability to fit with the globalisation permitted by technology.

491 For instance, the 'Legal' part of the MaxiMine whitepaper describes the legal status of blockchains, cryptocurrencies and ICO tokens for certain jurisdictions (China, United States, European Union, Australia and Singapore), *Maximine Whitepaper*, p. 37 ss, https://maximine.io/whitepaper/whitepaper_en.pdf; the Booking token Unit whitepaper's section on disclaimer provides for some legal information regarding the statute of cryptocurrency and ICO tokens according to European and French laws. It also submits the purchaser of the tokens to some obligations of French law, including some obligations whose breach is to be considered a criminal offence according to French law, V. CHRIQUI, H. HABABOU, *Whitepaper Booking Token Unit (BTU) Protocol*, cit., p. 21. See also, for example The Tokes platform whitepaper launching tokens related to the Cannabis industry limits the selling of tokens to jurisdictions where a legal cannabis industry exists and, it only provides for exchange of the tokens in exchange of cryptocurrency or U.S. Dollars, Tokes Platform, Whitepaper version 3.1, 2018, p. 27, https://tokesplatform.org/TokesPlatform_WhitePaper.pdf, which provides that « Tokes may not be resold to purchasers who are citizens or permanent resident of China, Singapore, New York or any other jurisdiction where the purchase of Tokes may be in violation of applicable laws (including but not limited to laws regulating controlled substances, such as cannabis) »

492 For instance, the MaxiMine Whitepaper has been published in several languages, including English and Chinese, *Maximine Whitepaper*, cit.

493 A. SEN, *Dix vérités sur la mondialisation*, in *Le Monde,* 2001, p. 1.

II.4

Seen the insufficiency of the regional response provided for by the Council of Europe Convention and its rules on jurisdiction, conscious of the difficulties faced by national jurisdiction rules, and above all conscious of the necessity for States to coordinate in order to prevent numerous positive conflicts of jurisdiction, scholars kept on looking for alternatives to territoriality. Some of the proposals made by scholars in order to develop jurisdiction rules that would better fit the cyberspace than the territoriality principle currently does will be reviewed in this paragraph. Most of those have been only made with regard to cybercrime and as a result, authors were not aware of the issues raised by blockchains (especially because most of the opinions were made before the quick and recent development of blockchains). While it is not the aim of this article to provide for a unique solution in order to tackle the issue of jurisdiction on blockchains, we will review some of the solutions proposed by scholars and see whether they might be applicable and desirable for the Blockchain environment.

One proposal would suppose that, even though the new challenges brought by the global character of the Internet cannot be denied, it is unlikely that it will lead to special jurisdictional rules if the Internet could adapt itself in order to impose fictional territorial borders within the cyberspace[494]. Thus, traditional jurisdiction rules based on territoriality may be adequate and sufficient to solve jurisdictional issues[495]. In the context of blockchains, we distinguished a beginning of such a development for private blockchains in the third section of the article when we analysed the possibility to apply the targeted public theory to private blockchains in order to establish jurisdiction. However, this may be more difficult when dealing with public blockchains which are by nature globally open and not subject to any restrictions that could be applied by any authority or third party.

In the context of jurisdiction in Internet disputes, a proposal was made in order to consider the cyberspace as a separate international space (such as it is the case for the high seas, the international space or the Antartica). According to this proposal, jurisdiction should be based on the nationality principle irrespective of the geographic location as it is already the case for the other international spaces, mentioned above[496]. This may be hardly manageable regarding blockchains, especially because it may be difficult to determine which person committed the offence. We should recall that a blockchain is by nature distributed. Since the approval of an additional transaction on a blockchain results from the actions of many actors, it may be difficult to isolate one person that would be responsible for an offence. Even if this proposal argued for the so called active nationality principle to establish jurisdiction (which refers to jurisdiction established according to the nationality of the offender), we could make a link between this proposal and the modifications made to the French criminal code in 2016 in order to solve the territorial issue of cybercrime[497] by adding article 113-2-1 according to which any crime realised by means of an electronic communication network which is committed against a person living in France, is to be considered as committed

494 T. SOLLEY, *The problem and the solution: using the Internet to resolve Internet copyright disputes*, cit., p. 834.
495 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 17 ss.
496 Proposal made in D. C. MENTHE, *Jurisdiction in cyberspace: a theory of international spaces*, cit.
497 Loi no. 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF n°0129, 4 June 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id.

within the territory of France. So, even if the offence had been committed somewhere else, if the victim is located in France, the offence should be considered as having been committed in France and thus, the French jurisdictions should be competent. This competence echoes the passive nationality principle (according to which a State may have jurisdiction over offences committed abroad when the victims are its nationals). This modification to the criminal code has been admitted by the French Council of State which considers that it responds to the Government's objective to secure and legally reinforce the proceedings in terms of cybercrime[498].

With regard to blockchains, if this passive nationality theory enables to overcome the difficulties that reside in the determination of the place of commission of the offence that are faced with active nationality theory, it may not solve all of the difficulties. As we already saw, the distributed character of the blockchains supposes that the effects of an offence, and the victim may be located in any jurisdiction where the blockchain is available.

Some scholars pleaded for a unification of national jurisdiction rules[499] that would consist in the introduction of a transnational criminal law, specific to the era of Internet[500]. In this respect, it is argued that the cyberspace should be considered a sovereign jurisdiction[501]. In this case, it would be necessary to take into consideration the characteristics of the cyberspace, especially the transnationality of the offences[502], in order to establish new rules that would correspond better to the global character of the Internet. In other areas of law, amongst other regarding Internet dispute resolution, some share this view and call for a Convention on Internet jurisdiction, which should be an effective strategy for ensuring legal certainty[503], predictability and enforceability. However, even though a common approach may be beneficial, it may not happen because of States' reluctance to do so and to abandon their sovereignty and jurisdictional claim over the Internet[504]. This reluctance has been highlighted in the area of copyrights law on the Internet[505] and it is even more important in the area of criminal law given the nature of the area and the sovereignty principle to which States are strongly attached.

498 Conseil d'Etat, *Avis sur un projet de loi renforçant la lutte contre le crime organisé et son financement*, l'efficacité et les garanties de la procédure pénale, N° 391004, 28 January 2016, http://www.conseil-etat.fr/content/download/54700/484379/version/1/file/391004%20EXTRAIT%20AG%20AVIS.pdf.

499 A. HUET, *Droit pénal international et internet*, Travaux du centre de recherche sur le droit des marchés et des investissements internationaux (eds.), *Souveraineté étatique et marchés internationaux à la fin du 20e siècle, Mélanges en l'honneur de Philippe Kahn*, Paris, 2000, p. 675 ss; L. XIAOBING, Q. YONGFENF, *Research on criminal jurisdiction of computer cybercrime*, in *Procedia Comput. Sci.*, 2018, p. 795; S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 2.

500 See for example A. HUET, *Droit pénal international et internet*, Travaux du centre de recherche sur le droit des marchés et des investissements internationaux (eds.), cit., p. 675 ss.

501 S. P. BEATTY, *Litigation in cyberspace: the current and future state of Internet jurisdiction*, cit., p. 139.

502 C. MEIER, *Vers un système judiciaire mieux adapté à la cybercriminalité*, p. 6, http://www.lecreis.org/colloques%20creis/2001/is01_actes_colloque/meier.htm.

503 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 19; R. DAVID, *The methods of unification*, in *AJCL*, p. 25, 1968, http://www.imeryurdaneta.com/archivos/clases/art_382__DAVID%20-%20The%20Methods%20of%20Unification.pdf.

504 See for example, J. FRANCILLON, *Cybercriminalité, aspect de droit pénal international*, cit.; D. J. B. SVANTESSON, *Borders on, or border around – The future of the Internet*, in *Alb. L.J. Sci. & Tech.*, 2006, p. 352.

505 T. SOLLEY, *The problem and the solution: using the Internet to resolve Internet copyright disputes*, cit., p. 834.

Other scholars rather argue for a harmonisation of national jurisdiction rules[506]. While unification would consist in a unique set of rules, directly applicable for State parties, harmonisation would focus more on developing more coherence between the different national jurisdiction rules by reducing the differences among them but while respecting their particularities. This may constitute a more reasonable solution because it would be more respectful of national sovereignty and States may therefore be less reluctant to such a proposal.

7. In criminal matters, the territoriality principle is used in order to determine that a State has jurisdiction over offences committed on its territory. The territoriality is strongly linked to the principle of national sovereignty which supposes that no State should interfere with the competence of another for offences committed on its territory. According to the ubiquity theory, the territorial principle is extended and it enables a State to prosecute any offence whose, at least, one of its constituent elements is located on its territory – including the effects of such an offence.

However, territoriality was challenged by the development of the Internet and by the phenomenon of cybercrime which accompanied it. Because of the multiplicity of its actors and because of the fact that the Internet makes content available simultaneously at an international level, it seems difficult to determine on which territory a cybercrime has been committed – either through the use of the subjective or objective territoriality principle and national jurisdiction rules that follow those principles. At the regional level, the Council of Europe published a Convention, providing for basic jurisdiction rules based on territoriality. Even if the Convention was a progress because of its regional character, it did not solve the issue of positive conflicts of jurisdiction and let State parties discuss among them in order to choose the most adequate jurisdiction when more than one has jurisdiction over an offence.

We saw that the development of blockchains and of the criminality that accompanies it raise similar questions to those that accompanied the development of the Internet. To determine which jurisdiction is competent over an offence committed through or facilitated by the use of a blockchain may be particularly difficult for public blockchains because of the multiplicity and global character of its actors but also because of the joint control the nodes exercise over the blockchain. This may be less complicated for private blockchains where the applicability of the jurisprudence focusing on the targeted public that had been developed to tackle cybercrime, could be envisaged. However, a global response in order to determine with certainty a competent jurisdiction is lacking and, since the consequence is constant positive conflicts of jurisdiction, this may endanger the principle of legal certainty and the principles of the rule of law.

Most scholars have different views on what the best option is to tackle the issue of jurisdiction over cybercrime. Some would rely on technology itself to reinstall national borders and keep the territorial principle the way it is. This may be feasible for private blockchains but could be more difficult for public ones. Some would give up jurisdiction based on territoriality and would rely solely on the nationality principle to establish jurisdiction over offences on the cyberspace. This may also involve difficulties because of the multiplicity of the actors and the joint control exercised

506 S. NILOUFER, *The proper basis for exercising jurisdiction in internet disputes: strengthening state boundaries or moving towards unification?*, cit., p. 25; Y. A. TIMOFEEVA, *Worldwide prescriptive jurisdiction in Internet content controversies: a comparative analysis*, in *Conn. J. Int'l L.*, 2005, p. 214.

by nodes over the system. Some others argued for unification or harmonisation of national rules of jurisdiction even though States may be reluctant to such proposals.

So far, we should stress the inadequacy of national jurisdiction rules to tackle the issue of criminality on blockchains and the need to rethink the territoriality principle. The response should be discussed at a global level in order to prevent positive conflicts of jurisdiction and thus, reinforce legal certainty and the principles of the rule of law. However, the form of this response should still be discussed and thought about.

LOREN JOLLY

Panel III - Digitization of Public Administration and Big Data: tools, challenges and prospects of the transition to a digitalized public administration

III.1

Automated administrative procedure and right of access to source code

SUMMARY: 1. Introduction. – 2. Automated procedure: preliminary remarks. – 3. Right to access: preliminary remarks. – 4. Automated procedure and right of access to the source code. – 5. Tentative conclusions.

1. The aim of this work is to reflect on how a classical instrument of administrative law, i.e. the right of access to administrative documents (ex article 22 law 241/90), can be exercised, in case of automated administrative procedures, with respect to the source code of a software, and to discuss a number of problems raised by this issue.

Firstly, I offer a reconstruction of essential elements of the automated procedure and of the classic right of access. Secondly, also based on the most recent Italian case law, I focus on some problematic issues, including a) whether the source code can be qualified as an administrative document according to access' regulation and b) whether the source code and the related software – as protected by the intellectual property laws – can be subject to the right of access. This case opens a more general discussion on the methodology and the extent of the automation of administrative decisions, and how to adapt, through the example of the right of access, classical legal tools to innovations due to IT technologies.

2. First of all, it should be noted that when we talk about automation, we are referring to an activity carried out by a computer. [507]

Therefore, automated administrative procedures may be defined as all the cases in which the machine replaces the Administration in decision making processes. [508]

The fact that computers replace men, or public servants in the case of the Administration, obviously does not mean that human action completely disappears. As explained by Pubusa[509], human intervention remains essential in order to initiate automated administrative procedures. The Public Administration decides what the computer should do and elaborates instructions in the form of a program, which is therefore an expression of a human decision – in this case, of a public decision enacted by the Administration.

"Program" is also a central concept in administrative procedures, being composed by instructions based on logical rules that together form the algorithm. Through the program's instructions, the machine is able to reproduce a set of logical steps which elaborate the decision

507 For a general reconstruction see R. BORRUSO, *Computer e diritto*, Milano, 1978.

508 There is a vast literature on this subject: cf. *ex multis* D. MARONGIU, *L'attività amministrativa automatizzata*, Sant'Arcangelo di Romagna, 2005. U. FANTIGROSSI, *L'automazione e la pubblica amministrazione*, Bologna, 1993. A. USAI, *Le elaborazioni possibili delle informazioni. I limiti alle decisioni amministrative automatiche*, in G. DUNI (edited by), *Dall'informatica amministrativa alla teleamministrazione*, Roma, 1992, p. 55 e ss., P. OTRANTO, *Decisione amministrativa e digitalizzazione della P.A.*, in *federalismi.it*, 2017. (cf. https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=35595&dpath=document&dfile=17012018100422.pdf&content=Decisione%2Bamministrativa%2Be%2Bdigitalizzazione%2Bdella%2Bp%2Ea%2E%2B-%2Bstato%2B-%2Bdottrina%2B-%2B).

509 Cf. F. PUBUSA, *Diritto di accesso e automazione, Profili giuridici e prospettive*, Milano, 2006.

(based on data already provided, *inputs*). We can already observe that the most complex issue consists in translating the law into an algorithm, since the "will" determining an administrative decision or a legal rule has to be both completely and correctly represented to be lawful. [510]

When debating the possibility of automating the administrative activity, we might first consider that the operation is not so hard. One could think that the automation of the administrative activity is anything different from an 'automatic' application of the law, the latter being the application of an abstract norm to a concrete case. Being 'automatic', this operation could easily be carried out by a program realized for that purpose (a series of inputs, which are elaborated according to the rules of the programme, should be provided to the machine).

As a matter of fact, it is a much more complex operation, requiring some specific precautions for the following reasons: firstly, because the law should always be interpreted[511]; secondly, because the relationship between law and administrative activity, and, ultimately, between the principle of legality and administrative action, is not clear cut. Indeed, the law can regulate the activity of the administration according to a principle of substantial legality and, thus, limit the options of the available political decisions of the Administration. On the contrary, the law could also allow leeway for the Administration and thus a margin of discretion in the discipline of the concrete case according to a principle of formal legality. In this second scenario, constituting an example of discretionary activity of the Administration, the latter has to make an assessment and balance involved interests. Of course, different possible outcomes could be reached in carrying this activity. Nevertheless, in case of administrative discretionary activity, there is the assumption that the Administration is in the best position to effectively assess and pursue the public interest. It follows that the automation of discretionary administrative activity is challenging: while the identification of public and private interests and the resulting various solutions could be performed by the machine, the choice of the best solution for the concrete case should a prerogative of the human being.[512]

The paper argues that the automation for the entirely administrative activity subject to the principle of substantive legality is possible, but poses some difficulties in relation to the interpretation of the applicable norm or the circumstances in which a rule, even if precisely and correctly interpreted, refers to indeterminate extra-legal concepts. Therefore, we can conclude that

510 Cf. D. MARONGIU, *L'attività amministrativa automatizzata*, p. 11: «A relevant problem is how communication between legal and IT experts should take place when the software is realized, if it is necessary to identify formal procedures when public servants communicate to the programmers, to guarantee a the perfect "translation" of the natural language to the programming language» (translation mine) [«una problematica posta in evidenza è come debba avvenire la comunicazione fra giuristi e tecnici informatici al momento dell'ideazione del *software*, se cioè occorra individuare procedura formali nel momento in cui i funzionari comunicano ai programmatori le determinazioni che dovranno essere assunte mediante automazione, a garanzia della perfetta "traduzione" del linguaggio naturale al linguaggio di programmazione»].

511 Cf. F. PUBUSA, *Diritto di accesso e automazione, Profili giuridici e prospettive*, cit. p. 139 ss. For a general reconstruction see G. SARTOR, *Le applicazioni giuridiche dell'intelligenza artificiale,* Milano, 1990.

512 In this paper we decided not to take into consideration evolution of the AI in reproducing human reasoning. See *ex* multis F. AMIGONI, V. SCHIAFFONATI, M. SOMALVICO*, Intelligenza artificiale,* in *Enciclopedia della scienza e della tecnica*, Roma, 2008, S. CIVITARESE MATTEUCCI, L. TORCHIA, *La tecnificazione*, in L. FERRARA, D. SORACE, *A 150 anni dall'unificazione amministrativa italiana.* vol. IV, , in *Inf. Dir.*, 2008.

there is a close link between the application of the principle of substantial legality to administrative activities and the potential for automation in administrative procedures.

3. It would be challenging to contain in one paper a thorough analysis of the entire set of rules governing the right of access in the Italian legal system: there is a vast literature on the subject, to which we refer. [513]

For the purposes of our discussion, it is more appropriate to consider selected aspects related to the exercise of this right, especially in light of the regulation introduced by the law no 15 of the 11th February 2005.

Within the law 241 of 1990, the right of access is placed at the end of the regulation of the administrative procedure. As such, it constitutes a tool to balance the need for celerity in the administrative action and the protection of those subjective legal positions. Law 241 provides devices to exert the public function with efficiency, efficacy, and cost saving, while at the same time offering suitable tools to protect private interests, either directly or indirectly. Specifically, it offers tools that license access, both in the course and at the conclusion of the procedure, to the documentation employed by the administration to evaluate private and public interests and reach the final decision. This cognitive accessibility is achieved through the right of access. In this respect, the right of access constitutes a relevant public interest to the effect that it is enforced nation-wide on the same level. The extent to which the right of access is licensed by the Constitution still constitutes, however, a matter of dispute. Whereas its connection with article 97 is uncontroversial, scholars and case law still discuss whether the right of access can also be connected with the right of information ex art. 21, or better with article 24. The latter is also grounded on the fact that full knowledge of the administrative action is the condition and grants the effectiveness of the judicial protection.

4. We can assume that there is the possibility that an automated administrative decision is vitiated by 'invalidity': indeed "the invalidity of an administrative act is a consequence of the act's non-conformity compared to its legal model, to the punctual regulation of its conditions, of its procedural rules and to the effects expected with its adoption". [514]

Since the early studies on the administrative automated procedures, scholars have observed that one of the main expectations arising from this new type of procedures was the potential significant reduction of invalidities of administrative acts (e.g. breach of the principle of impartial treatment). It is undeniable that this was a reasonable expectation. However, it is equally undeniable that new and unknown invalidities may occur precisely because of the automation: they could be

513 Cf. *ex multis*, L. MAZZAROLLI, *L'accesso ai documenti della Pubblica Amministrazione. Profili sostanziali*, Padova, 1998.

514 Continued: « […] The invalidity of an administrative act is a consequence of the non-conformity of the act to its legal model and to the punctual regulation of its conditions, of the effects and ways of the procedure for its adoption» (translation) [«l'invalidità di un atto amministrativo è conseguenza della non conformità dell'atto rispetto al suo modello legale ed alla regolamentazione puntuale dei suoi presupposti, dei sui effetti e dei modi di essere del procedimento previsto per la sua adozione»] Cf. A. Masucci, *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico a istanza di parte*, Milano, 2011, p. 107.

related to the instructions provided by the Administration, to wrong algorithms or software operations, or to the processing of the individual automated act. [515]

It is suggested that invalidities of administrative acts resulting from administrative automated procedures could be divided in two groups:

First, invalidities related to how the software's structure and operation. In this case, the invalidity would affect all acts adopted with the same program. Second, invalidities of individual automated acts.

In order to acknowledge the existence of invalidities of both traditional administrative decisions - adopted by administration employees and officials - and automated ones, it is necessary to have full knowledge of the relevant law (and therefore of instructions provided by the Administration for the program), and for the software's functioning itself.

The aim of this section is to investigate the relationship between automated procedure, right of access and the scope of the relevant judicial protection.

As a matter of fact, the right of access can be exercised for the purpose of a possible subsequent judicial protection. As a starting point, our analysis should focus on whether article 22 of the law 241/90, which provides the right to access, could apply in relation to an automated administrative procedure. Notably the question would be whether this provision could be applied to gain access to the programme used for the administrative procedure. Thus, the first issue would be what part of a programme could be accessed and whether there should be any limits attached to access.

In order to answer these questions, a case study could provide useful insights. Back in 2016, the Italian Ministry of Education, University and Research (MIUR) decided to instruct a private company to elaborate a ranking to determine the location on the national territory of newly-recruited teachers. Consequently, teachers were asked to fill in an online application according to the methods indicated in the order 241/2016, which identifies rules concerning the mobility of teaching staff for the 2016/2017.

A group of teachers appealed the decision of MIUR on grounds of alleged breach of the principle of fairness, and brought an action in order to have access to the source code of the software that produced the ranking. Following the request of access to the programme used by MIUR, the applicants were provided only with a generic description of the software's function but not the code itself. The Administration relied on two arguments:

515 Another interesting aspect, which goes beyond the scope of the present paper, is which kind of judicial control could be exerted on automatic decisions. see *ex multis* F. SAITTA, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo,* in *Rivista di diritto amministrativo elettronico,* 2003, A.G. OROFINO, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in *Foro amm*., 2002, p. 2257 e ss. See also the decision no. 152 of Consiglio di Stato, sez. VI, 7 February 1995: «the administrative act which relies on automated procedures is not different from the ordinary administrative one, and scrutiny over its validity does not differ from the general rules, which require, first, the assessment of whether the act and its effect conform to the applicable rules, and, second, whether the claimant has suffered an actual and direct damage from the alleged violation". Translation from "l'azione amministrativa che si avvalga dell'informatica non si differenzia in nessun modo da quella ordinaria, e lo schema logico - giuridico da applicare nel caso di sindacato giurisdizionale si identifica con quello generale che esige la verificazione della conformità dell'azione e dei suoi effetti alla norma che li disciplina, in relazione alla circostanziata denuncia, da parte del soggetto che invoca tale sindacato, di una lesione personale, diretta ed attuale».

a. The source code of the algorithm should not be qualified as an administrative document under article no. 22 of the law no. 241 of 1990 (d);

b. The source code and the related software constitute intellectual works and are protected by the intellectual property laws.

The first point to be addressed is whether the software can be qualified as an administrative document ex. art. 22 l. 241/90 (d). [516]

As a preliminary observation, it is worth pointing out that most scholars interpret letter. d) of article 22 (as modified by the law no. 15 of the 11th February 2005, see p. 2), providing for the notion of administrative document, in a considerably extensive way, in the light of the substantial administrative nature of the document rather than its origin. In fact, it is settled administrative case law that the criterion of the origin of the document itself is relative and can be rebutted. The only relevant fact is whether the document concerns an activity of public interest. Thus, also private law acts can be qualified as administrative when they pursue the public interest.

It is the *ratio* of the law (article 22) that must be investigated to identify its extensive scope: the aim is to make knowable every act that made a contribution to form the will of the administration (it is not surprising therefore that exclusion's cases from the right of access are specific disciplined by article 24 of law 241/1990).

Some scholars and the established case law[517] therefore consider relevant the document due to the information it contains. To this effect, the document would be the object of access because it is the only reliable instrument (compared to others, e.g. to an oral will expressed by a public servant) to verify the information held by the Administration.

In the light of the above, the following question arises: is legitimate the request of access to the source code of the software used by the Administration?

Many objections could be raised to an affirmative answer: first of all, the software, due to its nature, is not intelligible by the public servant, nor directly elaborated by him. Moreover, it may be argued that the Administration adopts ex ante its decisions, and, therefore, that the software plays an auxiliary role, merely reproducing the will of the Administration.

Nevertheless, two considerations should be carefully analysed: Firstly, it is through the software that the content of the decision is realized and subsequently applied. It cannot be considered a mere execution, since the software performs those passages which previously were responsibility of the public servant. Secondly, the discretionary choice of the Public Administration to employ innovative instruments (in this case, the choice to use a software to manage a procedure) cannot result in a limit and should not place obstacles to the accessibility of the administrative act or of the procedure used.

516 Cf. l. d) art. 22 l. 241/90: «For "administrative document", any graphic, photographic or electromagnetic representation or any other form of the content of acts, including internal acts or acts not related to a specific administrative procedure, held by a public administration and concerning activities of public interest, regardless of the public or private nature of their substantial discipline» (translation mine) [«per "documento amministrativo", ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale»].

517 See G. TARANTINI, *Pubblicità degli atti e diritto di accesso*, in B. CAVALLO (edited by), *procedimento amministrativo e diritto di accesso*, Napoli, 1993. G. ARENA, *l'accesso ai documenti amministrativi*, Bologna, 1991.

III.1

When examining the highlighted questions in relation to the MIUR case, the administrative court (Tar Lazio, III-bis section) has held, first, that the source code of the software used by the MIUR could be qualified as an "administrative document" under l. d) art. 22 l. 241/90. [518]
A second problematic issue raised by the Administration is related to the protection of the intellectual property of the software. This matter can open a more general discussion about the possibility for the Public Administration of choosing open source software or specifically produced by the Administration.

Leaving aside the question of why the Administration has chosen - legitimately or not - to resort to a company in order to implement the software, the matter remains as to whether the right of access can be denied due to the protection of the copyright of an intellectual work (we assume that the software integrates the requirements of creativity and originality that allow the IP protection).

The applicable provision in this context is article 24 of of law 241/90, regulating the exemptions of the right of access.

In this respect, it is worth mentioning that the aim of copyright protection legislation is to preserve the economic advantage from the author or for the owner. Yet, the economic advantage of the author or the owner can be balanced with the interest protected by the right of access. Notably, the administrative court in the MIUR case has observed: «Neither copyright nor intellectual property preclude basic reproduction, but preclude, instead, only a reproduction which allows economic exploitation. The access does not damage the right to the exclusive economic use of the work, since there is a duty to make appropriate use of the information obtained with the access to the “document”, that is exclusively a functional use to the interest claimed with the request for access. The interest is represented by the protection of the rights of the claimants, as this constitutes not only the function for which access is allowed, but, at the same time, also the limit of use of information obtained. Whoever obtains access will be directly liable to the software owner » (translation from original).[519]

Another ground used to justify the refusal of access by the Public Administration is article 6 of law 97/2016, where the limits to the civic access are identified, because letter c) indicates also the economic and commercial interests of a natural or legal person, including intellectual property, copyright and trade secrets. We do not have the possibility to reconstruct the civic access regulation here[520]: we can just observe how the constitutive differences between the so-called "documental" access ex article 22 of 241/90 and the civic access made the reference to civic access’ limits made

518 Tar Lazio, sez. III-bis del 22 March 2017 no. 3769.

519 «Né il diritto di autore né la proprietà intellettuale precludono la semplice riproduzione, ma precludono, invece, al massimo, soltanto la riproduzione che consenta uno sfruttamento economico e, non essendo l'accesso lesivo di tale diritto all'uso economico esclusivo dell'opera, l'ostensione deve essere consentita nelle forme richieste da parte dell'interessato, ossia della visione e dell'estrazione di copia, fermo restando che delle informazioni ottenute dovrà essere fatto un uso appropriato, ossia esclusivamente un uso funzionale all'interesse fatto valere con l'istanza di accesso che, per espressa allegazione della parte ricorrente, è rappresentato dalla tutela dei diritti dei propri affiliati, in quanto ciò costituisce non solo la funzione per cui è consentito l'accesso stesso, ma nello stesso tempo anche il limite di utilizzo dei dati appresi, con conseguente responsabilità diretta dell'avente diritto all'accesso nei confronti del titolare del software».

520 Cf. D.U. GALETTA, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del D. Lgs. n. 33/2013*, in *federalismi.it*, 2016.

by the Administration ineffective: indeed, in classical access – as seen in paragraph 2 – there is a direct interest in protecting a qualified legal position, which could justify higher knowledge.

5. In the MIUR case, the administrative court authorizes access to the software source code (related to the teachers' mobility procedure 2016/2017). Regardless of the solution adopted by the court and the effects[521] of this decision, some (tentative) conclusive remarks arise. First, it is useful to read the preliminary technical evaluation[522] carried out on the code after the access: it is of course a preliminary evaluation and it was made upon motion of a party (even if it raises some interesting issues on programming methods) but it suggests a central reflection. In the context of the technical evaluation, the experts assess how the way in which the code was provided does not allow to execute it and to test the functioning and it invalidates the order of extension of the court. [523] It could be argued that it is precisely the use of automation that makes more difficult to understand the functioning of the mobility procedure; in this way it would be carried out in fact the risk noted by the court: "the use of innovative tools by the administration for the management of its procedural activity [...] could produce a limit to the cognitive accessibility by the recipient of the act". Indeed, in our opinion, the problem does not arise in a different way when the access request is promoted towards a "classical" document. This leads to a more generic methodological consideration: instead of creating new tools in light of technological innovations, efforts should be made to adapt already existing notions.

In the second place, a comparative perspective is also required, in order to understand how other national legal systems have dealt with similar problems. Indeed, the case at hand is an excellent example of the need to assess at least the best practices on the European level (consider for instance the case of France and its regulation to access in case of automated administrative decisions). [524]

521 As a result of the mobility procedure, were presented a very large number of applications.

522 The preliminary technical evaluation (June 2017) was required by claimants on the software after the delivery by the Administration.

523«It is clear that the lack of clarifications, as well as the lack of the files indicated in the code, in the database, of the files that the software uses as well as the technical specifications, configures a conduct that is not transparent, despite the order of extension by the court. These omissions irreversibly affect the possibility of a complete control on the concrete work of the algorithm and, therefore, on the way in which it has determined the positions of teachers on the national territory» (translation mine) [«È evidente che la mancanza di tali precisazioni, così come la mancanza dei file richiamati all'interno del codice, del database, dei file che il software utilizza in lettura e scrittura dei dati (non tanto nei contenuti quanto nella forma) nonché delle specifiche tecniche, configura una condotta poco trasparente, nonostante l'intervenuto ordine di ostensione dei dati e degli atti da parte del TAR, nei confronti del Ministero. Tali omissioni inficiano in maniera irreversibile la possibilità di un completo controllo sulle concrete modalità di utilizzo dell'algoritmo e, quindi, sulle modalità che hanno determinato lo spostamento degli insegnanti sul territorio nazionale»], preliminary technical evaluation of the software 4 June 2017.

524 Decret no. 2017-330, March 2017.

III.1

A final note concerning the relationship between organizational autonomy and automated procedures. The assumption that the choice of the administration to automate its procedures lies within the administration's power has widely gone unchallenged. However, it is questionable whether this entail a certain degree of ambiguity, for example concerning the interpretation of the law, and whether a more uniform choice on the national level should be pursued instead.

GIULIA PINOTTI

III.2

The Algorithmic Governance of Administrative Decision-Making: Towards an Integrated European Framework for Public Accountability

SUMMARY: 1. Introduction and Outline of the Study- 2. Context and Features of the 'Algorithmized' Public Administration- 2.1 The Private-Public Partnerships for the Delivery of Algorithm-driven Public Services- 3. Legal Obstacles to Accountable Algorithmic Public Decision Making- 3.1. The Subjective Obstacle: the Unsuitability of Administrative Law Principles of Accountability and Transparency- 3.2 The Objective Obstacle: the Intellectual Property Protection of Privately-Developed Algorithms- 4. The General Data Protection tools of Transparency and Accountability- 5. Conclusions

1. The shift from a big data- to an algorithm-driven economy, currently changing the face of many private domains, is ultimately touching also upon the public sector. Here, the growing use of algorithms for the purposes of decision-making in the field of public services is sensitively transforming the way in which public action is carried out.

Examples of algorithm-driven public decisions are blossoming in the USA and are starting to become apparent also in the European Union. In the USA, for example, and more specifically in the city of New York, the local government has employed algorithms in order to carry out the most various activities, ranging from the allocation of police officers, firehouses, public housing, food stamps[525]. Also within European Union Member States, examples of algorithmic employment in the public sector are proliferating. In these regards, mention must be made of the practice of profiling the unemployed done by the Ministry of Labour and Social Policy in Poland[526]. In France, with the declaration of the state of emergency after the last terror attacks, the police has started employing a software that predicts where and when crime is going to occur[527]. Also the Dutch tax authority is relying on algorithm-driven correlations to increase the efficiency of the tax system[528].

All these examples show that the enhancement of computational capabilities is structurally changing the ways in which public services are delivered. This paper moves from this acknowledgment and enquires the legal pitfalls of this newly emerging scenario from a European Union law standpoint.

Against this backdrop, the paper is structured into two sections.

525 J. Powles, *New York City's Bold, Flawed Attempt to Make Algorithms Accountable*, published on the 20th December 2017 on the New Yorker, online available at https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable.

526 This is documented by J. Niklas, K. Sztandar-Sztanderska, K. Szymielewicz, *Profiling the unemployed in Poland: Social and Political Implications of Algorithmic Decision-making*, 2015, online available at https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf, *passim*.

527 K. Kubler, *Surveillance, Power and Algorithms in France's State of Emergency*, in *Big Data & Society*, July-December 2017, p. 1 ff..

528 C. Quelle, *Privacy, Proceduralism and Self-Regulation in Data Protection Law*, in *Teoria Critica della Regolazione Sociale*, 2017, p. 3.

The first section illustrates the features of the 'algorithmized' public administration, showing how the increasing reliance on data-driven systems, obliges the public sector to lean on private companies' technical expertise and infrastructure. In light of the peculiarities of the emerging environment, the second section will enquire the (in)effectiveness of traditional European administrative law tools in respect to accountability objectives. Hence, the analysis will turn to the consideration of the new provisions of the General Data Protection Regulation. The study will conclude with some systemic considerations regarding the need to adopt an integrated approach between traditional administrative law tools and business-centred provisions entailed in the GDPR.

2. Algorithm-driven decision-making has first proliferated in the private sector where it has become the major business model in so-called digital markets, exploiting users' personal data for commercial purposes- *i.e.* is primarily for predicting and thus orienting users' commercial behaviour- and thus with the primary aim of maximising companies' profits[529]. The employment of such massive processing techniques in the public sector has come behind and has sensitively different features and outcomes in respect to the private and commercial-oriented sphere.

Lately, algorithmic processing infrastructures have triggered governments' attention that have over time become large depositories of citizens' personal data[530]. The digitisation of public administrations' databases has soon enabled a faster consultation of collected and available datasets.

These patterns have been amplified with the increasing employment of algorithms as processing infrastructures of public administrations' collected data. Through processing algorithms, data are not any more a static evidence merely working as a support of public decision making carried out by public officials, but have themselves become, in those sectors where algorithms are employed, the centre and the source of decision-making[531].

The increasing quantitative and qualitative importance of algorithms for the purposes of decision making in various fields of the public sector is transforming algorithms into outright governance tools: algorithms are indeed employed as a means for authorities to manage "individual behaviour and allocate resources" It thus appears that, similarly to the private sector, also the public sector is being overtaken by a new form of algorithmic governance[532].

Through the 'algorithmisation' of public action, public affairs begin to be regarded as technical problems that need to be addressed through technical solutions[533]. With algorithms becoming the engines of public affairs' management, and thus exerting control over society[534], a new form of technocratic public governance emerges, apparently providing impartial and scientifically-grounded decisions on the basis of data-driven models. These data-driven models are

529 G. Comandè, *The Rotting Meat Error: From Galielo to Aristotele in Data Mining?*, in *EDPL*, 2018, 4, 3, p. 270.

530 G. Carullo, *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e Mercato*, 2016, 23, p. 181 ff..

531 K. Yeung, *Algorithmic Regulation: a Critical Interrogation*, in *Regulation & Governance*, July 2017, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505, p. 20 ff..

532 The term 'algorithmic regulation' was first coined by T. O'Reilly, *Open Data and Algorithmic Regulation*, in B. Goldstein, L. Dyson (ed.), *Beyond Transparency - Open Data and the Future of Civic Innovation*, San Francisco, 2013, p. 289-300.

533 R. Kitchin, *The real-time city? Big data and smart urbanism*, in *GeoJournal*, 2014, 79, 1, p. 9.

534 M. Janssen, G. Kuk, *The Challenges and Limits of Big Data Algorithms in Technocratic Governance*, in *Gov. inform q.*, 2016, 33, p. 371.

ultimately creating a new form of "technological determinism" given by algorithms' predictions triggering public action[535]. Algorithms indeed rely on "actuarial predictions" given by the correlations between the features or characteristics drawn from the data[536]. As framed in these terms, the "algorithmised" public governance is drastically overturning the traditional manners of conduction of public affairs[537], ordinarily based on what some strand of the literature has called "clinical predictions", consisting in public officials' management of specific situations[538].

Conversely, in the current technological environment, the human evaluative factor is increasingly being replaced by machine-driven calculations[539]. Hence, in respect to these automated processing systems and the readily usable knowledge they generate, public administrations and public officials specifically in charge of exercising public action become mere executors of evaluations entirely carried out through automated systems. In other terms, algorithms are being deferred the substantial part of the decision-making process, whereas public officials maintain only the function of formalising and practically enacting judgements taken by the machine-driven model.

2.1. Governments' technical limitations make private contractors key components of data-driven decision making processes[540]. The technological support provided by private corporations has thus become of primary importance for addressing the public need in an era of technological disruption, and thus for acquiring the analytics necessary for "smart" urban systems.

The outsourcing of processing infrastructures needed for the handling of the enormous available datasets is formally occurring through public-private partnerships[541], which have been defined in the literature as "any arrangement between government and the private sector in which partially or traditionally public activities are performed by the private sector"[542].

These private-public partnerships create a bi-directional flow of datasets that benefits both the private and the public stakeholders involved. Indeed, through these service contracts, publicly owned data flow into the processing infrastructures offered by private companies. In this way, these companies acquire control of such data, which thus come to aliment and thus enrich their processing

535K. Yeung, *Algorithmic Reguation: a Critical Interrogation*, cit. p. 20.

536 R. Brauneis, E.P. Goodman, *Algorithmic Transparency for the Smart City,* in *YJoLT*, 2018, 103, p. 111 ff..

537 M. Tenney, R. Sieber, *Data-Driven Participation: Algorithms, Cities, Citizens, and Corporate Control*, in *Urban Planning*, 2016, 1, 2, p. 101 ff..

538 R. Brauneis, E.P. Goodman, *Algorithmic Transparency for the Smart City,* cit. p. 111 ff..

539 This is the general definition of governance given by J. Black, (2014) *Learning from Regulatory Disasters*. LSE Law, Society & Economy Working Papers 24/2014, online available at http://eprints.lse.ac.uk/60569/1/WPS2014-24_Black.pdf.

540 T. Filer, *Developing AI for Government: What Role and Limits for the Private Sector?,* online available at https://www.bennettinstitute.cam.ac.uk/blog/developing-ai-government-what-role-and-limits-priv/. For a general assessment, see P. Vincent-Jones, *The Regulation of Contractualization in Quasi-Markets for Public Services*, in *Pub. L.*, 1999, p. 304.

541 For a deeper assessment over the issue of private-public partnerships, although specifically focused on the police sector, see N. Purtova, *Between GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private Partnerships*, in *IDPL*, 2018, 8, 1, p. 52 ff..

542 E.S. Savas, *Privatization and Public-Private Partnerships*, Chatham House, 2000, 4. See also European Commission, *Green Paper on Public-Private Partnerships and Community Law on Public Contracts and Concessions*, April 2004, p. 9.

systems[543]. On the other side, private corporations' data- and the information they entail-, originally feeding the provided algorithmic infrastructure, become equally relevant for the purposes of public actors: this privately-owned data that has originally trained the algorithmic model has a sensitive impact on the results rendered by the processing system; it is thus this data that ultimately defines public decision-making. In addition to this, governments also often make specific agreements for accessing privately held data in order to strengthen the evidence given by public datasets[544]. The agreements specifically designed for the transfer of datasets from private actors to public bodies often accompany the private-public partnerships aimed at providing the processing infrastructure[545].

The proliferation of private-public partnerships for the allocation of "algorithmised" public services are giving rise to an interesting process of infiltration of market rationales in the determination of public actions' courses. With privately-constructed algorithms shaping public interventions, private corporations are gaining an increasing important role in the organization and orientation of the public sector[546]. The related spillover effect is that the growing involvement of private corporations in public affairs causes the marketization of public services given that corporations increasingly provide these processing services to public actors in order to increase their profits. This phenomenon has been elsewhere called 'corporisation' of city governance[547], bringing about the risk of corporate capture of public power[548].

The delegation of the decision making site governing the allocation of public services to private actors requires a robust regulation and a strong enforcement in order to avoid an uncontrolled interference of the technology sector in public matters: with the rise of public-private partnerships for the machine-driven delivery of public services, governments' accountability results to be intrinsically connected to- and thus depends on- the transparency of companies' processing activities.

3. The above-outlined paragraphs have shown how the rising employment of algorithms in the public sector is sensitively transforming the dynamics of public decision-making.

The increasing involvement and role of private informational and technological assets in the delivery of public services has two main effects. On the one hand, indeed, it "neutralizes" the administrative law rules of accountability and transparency that traditionally guard the traceability of public administrations' actions. This occurs because these rules only apply to public administrations- that, as illustrated above, are emptied by algorithms of substantial decision making functions-, and thus cannot be applied to private contractors (*subjective obstacle*).On the other hand,

543 See L. Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, in *EDPL*, 2016, 2, p. 28-58.

544 For an analysis regarding government access of privately held data in the UK, see I. Brown, *Government Access to Private Sector Data in the United Kingdom*, in *IDPL*, 2012, 2, 4, p. 230 ff..

545 F.H. Cate, J.X. Dempsey, I.S. Rubinstein, *Systematic Government Access to Private-sector Data*, in *IDPL*, 2012, 2, 4, p. 195 ff..

546 R. Brauneis, E.P. Goodman, *Algorithmic Transparency for the Smart City*, cit. p. 114, where the Authors recall the registration by IBM of the trademark 'smart city".

547 R. Kitchin, *The real-time city? Big data and smart urbanism.*, cit. p. 5. See also J.S. Hiller, J. M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, in *Hastings L.J.*, 2017, 68, p. 309.

548 R. Brauneis, E.P.Goodman, *Algorithmic Transparency for the Smart City*, in *YJoLT*, 2018, 103, p. 20. See L. Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective,* cit. p. 32.

conversely, it operationalizes the whole set of intellectual property tools that companies have at their disposal in order to protect the products of their technological research & development, thus raising substantial barriers for public administrations that turn out to be incapable of accessing the logic underlying the privately-originated machine-driven processes (*objective obstacle*).
These two points will be enquired in the following paragraphs.

3.1. The private algorithmic processing infrastructures to which public bodies are increasingly resorting and the private-public partnerships that govern the transfer of such technology call into question some fundamental principles that rule both the political and administrative action, and more precisely the ones related to the accountability and the transparency of public administrations' action. These principles are foundational principles of good governance[549].

The notion of public accountability relates to the political legitimacy of public institutions in democratic systems. More precisely, public institutions' political legitimacy implies a responsabilization of these same institutions in the sense that their actions have to satisfy the public mandate received and that they have to signal such compliance to the citizens who bear the effects of public actions. In this perspective accountability contributes to strengthening the principle of democracy as expressed in art. 6 of the European Treaty and in the Charter of Fundamental Rights of the European Union.

In these regards, it is interesting to recall that the 1998 OECD Principles for managing Ethics in Public Services explicitly acknowledges the principle of accountability, stating that "public servants should be accountable for their actions to their superiors and, more broadly, to the public. Accountability should focus both on compliance with rules and ethical principles and on achievement of results (…)"[550]. Along these lines, also the European Commission's White Paper on European Governance stresses the need for clarity with regards to "the roles in the legislative and executive processes" as well as the need for European institutions to "explain and take responsibility" for their actions[551]. Accordingly, the Paper affirms the "need for greater clarity and responsibility from Member States and all those involved in developing and implementing EU policy at whatever level"[552].

Against this backdrop, accountability implies openness of public authorities' interventions, requiring institutions and administrative bodies and agencies to open their activities to the public[553]. The principle of openness not only requires these actors to conduct their work as openly as possible, but also to proactively open their operations to the public. As will be assessed below, administrative

549 C. Harlow, *Global Administrative Law: the Quest for Principles and Values*, in the *EJIL*, 2006, 17, 1, p. 187 ff..
550 OECD, *1998 Recommendation of the OECD Council on Improving Ethical Conduct in the Public Service, including Principles for Managing Ethics in the Public Service*, online available at http://www.oecd.org/gov/ethics/Principles-on-Managing-Ethics-in-the-Public-Service.pdf, p. 76.
551 European Commission, *European Governance- A White Paper*, 25 July 2001, online available at https://ec.europa.eu/europeaid/sites/devco/files/communication-white-paper-governance-com200142820010725_en.pdf, p. 10.
552 *Ibid.*.
553 In these regards, see A. Alemanno, *Unpacking the Principle of Openness in EU law- Transparency, Participation and Democracy*, in *European Law Review*, 2014, 39, 1, p. 72.

openness has an instrumental value for it ensures the participation of civil society in public decision-making and with that the more fruitful enactment of democratic ideals.

Against this backdrop, the principle of accountability is intimately connected to the principle of transparency[554], which is explicitly acknowledged in art. 41.2 of the Charter of Fundamental Rights as part to the right of good administration, requiring institutions to "maintain an open, transparent and regular dialogue with representative associations and civil society".

The principle of transparency is enshrined in art. 15.3 TFEU, providing substantive and procedural rules for the operationalization of such principle. Transparency is highly context-dependent and thus varies depending on the activities that are carried out[555]. The public information released must be up to date, complete- that is, ready for consultation-, and consistent with the original documents held by the administration. It moreover needs to contain the indication of its origin and of how it can be reused.

The quality of transparency is strictly related to the administrations' use of a clear and understandable language of the information posted on the institutional channels of information. The requirement of a clear and plane language of the public information released to the public has been widely acknowledged by the case law of the Court of Justice of the European Union[556], which has stressed that clarity of language in the documents of the public institutions is strictly related to the principles of legal certainty and the protection of legitimate expectations. In these terms, transparency enables the predictability of policy action and is thus the more important the more the specific public action is the result of discretionary powers[557].

Public transparency's golden rule is given by the right of access to public documents, enshrined in art. 15 TFEU, in art. 42 of the ECHR, and in Regulation EC N. 1049/2001 of the European Parliament and of the Council on public access to EU institution documents[558].

As objectified in the right to access, transparency is itself functional to the right of defence and thus directly serves due process rationales[559]. This is well expressed in art. 41 ECHR defining the components of the right to good administration, entailing according to para 2 of the same article i) citizens' right to defence and due process, ii) the right to access to administrative documents and iii) the right to receive explanations regarding public actions.

554 For a theoretical reconstruction, see C. Harlow, *Global Administrative Law: the Quest for Principles and Values*, cit. p.187 ff..

555 *Ibid.*.

556 See, for example, Court of Justice of the European Union, *Administration des douanes v Société anonyme Gondrand Frères and Société anonyme Garancini,* C-169/80, 9 July 1981, online available at http://curia.europa.eu/juris/showPdf.jsf?text=&docid=90884&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=319462, para 17; Court of Justice of the European Union, *Amministrazione delle finanze dello Stato v Srl Meridionale Industria Salumi and others* and *Ditta Italo Orlandi & Figlio and Ditta Vincenzo Divella v Amministrazione delle finanze dello Stato,* C-212/80, 12 November 1981, online avalable at http://curia.europa.eu/juris/showPdf.jsf?text=&docid=91124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=321098.

557 S. Prechal, M. de Leeuw, *Dimensions of Transparency: the Building Blocks for a new Legal Principle?*, in *REALaw*, 2007, 1, p. 51 ff.

558 So art. 2 para 1 of the Regulation EC N. 1049/2001 of the European Parliament and of the Council on public access to EU institution documents.

559 In these regards, see S. Prechal, M. de Leeuw, *Dimensions of Transparency: the Building Blocks for a new Legal Principle?*, cit. p. 55.

III.2

According to the interpretation given by the literature[560], art. 298.1 TFEU, by stating that "the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration", extends the principles of accountability and transparency to the entirety of EU administrations, *i.e.* the administrations that act within the territory of the European Union[561].

The emergence of a horizontal chain of stakeholders governing public decision-making courses relying on algorithmic processing infrastructures sensitively challenges the above-outlined framework[562]. As has been demonstrated, indeed, in the networked algorithmised public decision-making environment, the role of the public authority is lessened and substantially substituted by private companies who do not have the typical democratic accountability requirements that, in a representative democracy, traditionally belong to public administrations[563]. Private entities contracting with public authorities for the purposes of delivering algorithmic processing infrastructures are not subject to the accountability and transparency requirements of public subjects. These entities can indeed hardly be considered as "bodies governed by public law", since the definition of such notion under art. 1.9 Directive 2004/18/EC excludes the industrial or commercial character of these bodies[564]. To the contrary, the entities that provide algorithmic processing infrastructures as a support to public authorities' decision-making mostly have a strong commercial and industrial characterization.

Against this backdrop, hence, the achievement of public accountability and transparency in the illustrated terms appears to be primarily obstructed by a subjective obstacle, that is the inapplicability of the principles of good administrative governance to the private entities that are progressively taking the reins of such governance. This means that in the networked algorithmic environment accountability of the public authority diminishes. As a consequence, control of the policy address through traditional administrative law tools becomes less effective.

560 A. Alemanno, *Unpacking the Principle of Openness in EU law- Transparency, Participation and Democracy,* cit. 72.

561 For the notion of EU administrations, see H. Hoffman, G. Rowe, A. Turk, *Administrative Law & Policy of the European Union*, Oxford, 2012, p. 171 ff..

562 For an empirical analysis of the challenges to democratic accountability posed by the contracting activities of public administrations with private entities, see C. Di Martino, J. Scott, *Private Sector Contracting and Democratic Accountability*, in *Educational Policy*, 2012, p. 1 ff..

563 On the issue see P.R. Verkuil, *Public Law Limitations on Privatisation of Government Functions*, Cardozo Legal Studies Research Paper N. 104, 1 March 2005, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=681517, p. 8, affirming that "delegations to private hands in our society come with strings attached that ensure fairness at the individual level and accountability at the political level".

564 Conversely, according to art.1.9 Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public work contracts, public supply contracts and public service contracts, "(…) a body governed by public law means any body: (a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; (b) having legal personality; and (c) financed, for the most part, by the State, regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law". The provision thus clearly excludes the industrial or commercial nature of the contracting entities in order to be considered a body governed by public law.

In addition to this, public administrations relying on privately-developed algorithmic models are themselves incapable of accessing the information needed to satisfy normative transparency and thus accountability requirements because of the existence of a strong set of intellectual property tools, which run contrary to transparency duties and thus to the enactment of effective public accountability mechanisms.

3.2. The European intellectual property framework provides several tools for the protection of corporations' developed algorithms. These are to be found in copyright, database rights and trade secret rights.

Although there have been long discussions regarding the patentability of "computer implemented inventions" [565], the option of patenting softwares has soon been put aside, due to the legal and practical difficulties related to such an extension[566]. The exclusion of the eligibility of the patent as a tool for the protection of algorithms has caused the shift of focus onto other tools of protection.

With regards to copyright protection, the Directive on the legal protection of computers of 2009[567], replacing the previous 1991 Software Directive[568], has redefined the scope of copyright protection of computer programs. The persisting uncertainties around such forms of protection have triggered the intervention of the European Court of Justice in the case *Sas Institute Inc. c. World Programming Ltd*[569]. Here, the Court has clarified that the protection under copyright law of computer programs applies only to "the forms of expression of a computer program and the preparatory design work capable of leading, respectively, to the reproduction or the subsequent creation of such a program[570]", but does not include the functionalities, the programming language of the program, and the format of data files used in a computer of it[571]. By stating so, the European

565 Cf. *Proposal of a directive of the European Parliament and of the Council related to the patentability of computer implemented inventions*, released on the 20th February 2002, online available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52002PC0092. See J Drexl, RM Hilty et. al., *Data ownership and access to data, Position statement of the Max Planck Institute for Innovation and Competition of the 16th August 2016 on the Current European Debate*, Max Planck Institute for Innovation and Competition Research Paper No. 16-10, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165, p. 5-6, stressing that patent "protection (of algorithms) would pose a risk of two negative effects: first, protection of abstract subject-matter would cause needless – and, in the case of algorithms, unreasonable – restraints on competition that, according to current knowledge, would not be economically justified. (…) Second, it is barely foreseeable what markets and sectors would be affected. This makes finding suitable approaches to a regulation seem unrealistic".

566 The Supreme Court of the United States, in *Alice Corp. v. CLS Bank International*, clarified that abstract inventions, such as algorithms, do not become patentable merely because they are implemented on a computer. So *Alice Corp. Pty. V. CLS Bank Int'l*, 134 S. Ct. 234, 2358 (2014). For a comment see Nicholson Price II, *Expired Patents, Trade Secrets and Stymied Competition,* cit. p. 1425.

567 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L. 111, 5-5-2009.

568 See Council Directive of 14 May 1991 on the legal protection of computer programs, 91/250/EEC, OJ 17-5-91, N.L. 122/42.

569 Court of Justice of the European Union, *Sas Institute Inc. c. World Programming Ltd*., C-406/10, 2 May 2010, online available at http://curia.europa.eu/juris/document/document.jsf?docid=122362&doclang=EN.

570 *Ibid.*, para 37.

571 *Ibid*., para 39. For a comment, see P. Samuelson, T. Vinje, W. Cornish, *Does Copyright Protection Under the EU Software* Directive *Extend to Computer Program Behaviour, Languages and Interfaces?,* in *EIPR*, 2012, 34, 3, p. 158.

Court of Justice has reaffirmed the basic copyright law principle on the basis of which copyrights protects only the original expression of an idea[572].

Through licensing terms, copyright protection can be used in order to restrict the ability of a third party to use the protected parts of the computer program. Indeed, in case the licenses are established through valid contracts, uses that do not respect the license terms may constitute breach of contract. Hence, copyright protection of algorithms has an important restrictive function regarding the use of the protected technology[573]. This means that copyright restrictions can well be used for impeding governments to employ the provided algorithms for purposes that are different from the ones indicated in the licensing terms.

Shifting from the processing infrastructure to the object of the processing, copyright can be employed for the protection of aggregated digital data processed by algorithms[574] in case the selection and arrangement of it meets the originality threshold[575].

Irrespectively of any inventiveness, digital datasets can find protection under the 1996 Directive on legal protection of databases[576], establishing an exclusive *sui generis* right over databases resulting from a "substantial investment"[577].

However, the strongest tool of protection that algorithms' developers have is trade secret protection as recently reformed by the Trade Secret Directive 2016/943. The new Directive provides indeed very broad conditions for protection, encompassing nearly every business confidential information[578]. Despite formal declarations[579], the Directive provides a proprietary-styled protection over information[580], which thus offers strong grounds for big data companies to obscure both the

572 See J. Litman, P. Samuelson, *The Copyright Principles Project: Directions for Reform*, in *BTLJ*, 2010, 25, p. 1190-1191.

573 Highlighting the function of copyright as a means to restrictively regulate the use of the protected object, N. Shemtov, *Beyond the Code: Protection of non-Textual Features of Softwares*, Oxford, 2017, p. 151.

574 For a reflection upon the copyrightability of so-called computer-generated works, see R. Abbott, *Artificial Intelligence, Big Data and Intellectual Property*: *Protecting Computer-Generated Works in the United Kingdom*, in T. Aplin (ed.), *Research Handbook on Intellectual Property and Digital Technologies*, forthcoming, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064213.

575 It should be however recalled that it is very difficult for a database to accomplish the originality threshold required under European copyright law. On the issue see DJ Gervais, *The internationalisation of Intellectual Property: New challenges from the very old and the very new*, in *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2002, 12, p. 929-935.

576 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal Protection of Databases, online available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML.

577 Cf. art 7, 4 par. Database Directive. Recently, see I. Gupta, *Footprint of Feist in European Database Directive: a Legal Anaysis of IP making in Europe*, Springer, 2017, p. 11-37.

578 See art. 2 of the Directive where trade secrets are defined as any information that i) is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; ii) has commercial value because it is secret; and iii) has been subject to reasonable steps to keep it secret. See D. Sousa Silva, *What exactly is a trade Secret under the proposed Directive*?, in *JIPLP,* 2014, 9, p. 11-15.

579 See recital 10 of the Directive affirming that its "provisions (...) should not create any exclusive right on the know-how or information protected as trade secrets"

580 Trade secret protection and enforcement is confined to cases of conducts of "acquisition, use and disclosure" that are to be considered "unlawful". The notion of unlawfulness is very broad and comprehends also any "unauthorised access to, appropriation of, or copy of any documents, objects, materials, substances or electronic files (…) containing

processed health data and the procedural information regarding algorithm-driven processing activities. This procedural information encompasses information regarding how algorithms are developed, how they are validated and the data on which they are trained[581].

The above-outlined intellectual property tools not only shield corporations' algorithmic assets from the eyes of competitors, but, in the dynamic of public-private partnerships, end up creating a substantial safeguard also in respect to the public counterpart[582]. Indeed, these tools and the contractual restrictions regarding them, block public contractors' access to the functional logic of the algorithms they get to employ, with the ultimate effect of rendering these same public administrations incapable of releasing to the wider public explanations regarding the process of the formation of public administrations' will.

In these regards, it is interesting to recall that access to document rules, such as the ones entailed in art. 41 ECHR, in art. 15 TFEU and in Regulation EC N. 1049/2001 regarding public access to European institutions documents provide specific exemptions with regards to the disclosure of those documents that "would undermine the protection of the commercial interests of a natural or legal person"[583]. The protection of business secrets has been recognised by the Court of Justice of the European Union as a general principle applicable in the context of public procurement[584]. Accordingly, these commercial confidentiality exemptions have been interpreted by the Court of Justice of the European Union in a very broad way[585] and also the latest rulings in these regards have confirmed the existence of an outright presumption of confidentiality in the case law of the Court of Justice of the European Union regarding access to public documents[586].

The obscurity of algorithmic decision-making courses renders it arduous for citizens to assert a claim of a right or a legitimate interest. Algorithms' intrinsic and extrinsic obscurity impedes a direct participation of citizens in machine-driven decisions carried out by governments.

the trade secret (…)" carried out "without the consent of the trade secret holder". See artt. 4 n. 56 and 6 of the EU Trade Secret Directive. See EU Directorate General for Internal Policies, *Trade Secrets*, 2014, online available at http://www.europarl.europa.eu/RegData/etudes/note/join/2014/493055/IPOL-JURI_NT(2014)493055_EN.pdf, p. 4; T Aplin, *Right to Property and Trade Secrets*, in C. Geiger, *Research Handbook on Human Rights and Intellectual Property* Cheltenham, 2015, p. 421-426.

581 All this information regarding algorithms constitute the so-called 'e-trade secrets'. R. Niebel, L. De Martinis, B. Clark, *The Eu Trade Secrets Directive: all change for trade secret protection in Europe?*, in *JIPLP*, 2018, p. 3.

582 D.S. Levine, *Secrecy and Unaccountability in Our Public Infrastructure*, in *Florida Law Review*, 200, 59, p. 149.

583 So art. 4.2 EU Access Regulation.

584 Court of Justice of the European Union, Case C-450/06, *Varec SA v. Belgian State*, 14 February 2008; online available at http://curia.europa.eu/juris/liste.jsf?language=en&num=c-450/06,para 49; Opinion of AG Kokott of 23 September 2010 in *Stichting Natuur en Milieu and Others*, C-266/09, online available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CC0266, para 77.

585 For the American perspective, see D.S. Levine, *The Impact of Trade Secrecy on Public Transparency*, in R.C. Dreyfuss, K.J. Stranburg, *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*, Cheltenham, 2011, p. 406 ff.

586 See, for example, Court of Justice of the European Union, Case C-562/14 P, *Sweden v. Commission*, 11th May 2017, online available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dc33afe3f799b84a4e9ab3c8c36aca0434.e34KaxiLc3eQc40LaxqMbN4Pb3uPe0?text=&docid=190582&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=715713. In the same sense, Court of Justice of the European Union, Case C-139/07, *Commission v. Technische Glaswerke Ilmenau*, online available at http://curia.europa.eu/juris/liste.jsf?language=en&num=c-139/07.

In this perspective, the opaqueness of privately developed algorithms implemented at governmental level brings about public disempowerment and loss of accountability. In respect to obscure algorithm-driven decisions shaping public interventions, citizens lose their participatory rights in collective ruling and become passive recipients of machines' determinations[587]. Against this backdrop, the acknowledgment of the unsuitability of traditional administrative "command and control regulation", suggests the need to look for new regulatory tools and governance mechanisms that are better capable of addressing the complexity of emerging algorithm-driven administrative decision-making patterns. The fact that algorithms who drive governments' decisions are privately controlled requires a shift in terms of systemic perspectives and thus of the tools needed to effectively pursue the accountability and transparency objectives. These tools are to be found in the General Data Protection Regulation, which provides specific tools with the aim of achieving accountability and transparency of algorithmic decision-making courses. As will be assessed in the following paragraph, these tools acquire a specific relevance for public accountability and transparency purposes in the "algorithmised" public environment.

4. In the effort to provide constructive regulatory responses to the phenomenon of massive machine-driven data processing, the General Data Protection Regulation has newly emphasized and reinvigorated the principles of accountability and transparency in the realm of data protection law. In this way, the two principles have acquired a new significance for the protection of data subjects' rights in the context of algorithmic processing activities.

The Regulation establishes an entire set of obligations born by entities that carry out personal data processing activities "wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"[588]. The Regulation applies to both private and public entities. This reflected by recital 6, acknowledging that "technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities"; as well as by the definition of "controllers" and "processors" under art. 4.7 and 4.8 GDPR, encompassing a "natural or legal person, public authority, agency or other body". In light of these provisions, it seems that for the purposes of the Regulation, private and public entities are generally equalized[589].

There are only a few regulatory differences between public and private actors[590]. The most significant relates to the requirement of the appointment of a data protection officer[591], always compulsory for public authorities and only compulsory for private entities if their core activities "consist of processing operations which, by virtue of their nature, their scope and/or their purposes,

587 *Ibid*..

588 So art. 2.1 GDPR, defining the "material scope" of the Regulation.

589 However, as Recital 19 GDPR clarifies that the processing activities carried out by public authorities for the purposes of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data" falls outside the specific scope of the Regulation.

590 In these regards, see O. Butler, *Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide*, in *European Public Law*, 2018, 24, 3, p. 555 ff..

591 Art. 37 GDPR.

require regular and systematic monitoring of data subjects on a large scale" or "of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10"[592].

Under these premises, the GDPR becomes a highly important source of regulation of the conduct of public administrations that make use of algorithmic processing infrastructures for the purposes of public services' delivery[593].

However, the GDPR's regulatory potential for public authorities' algorithm-driven decision-making is to be perceived also from a different, *indirect* or *subsidiary*, perspective: by regulating private corporations' processing endeavors, the GDPR's provisions assure as a reflex the enhancement of the accountability and the transparency of public authorities actions that are defined by privately-generated algorithms.

Under these premises, it is extremely interesting to observe that the regulation of data processing activities enacted by the GDPR is achieved through reliance on the same foundational principles regulating public administrations' acts, *i.e.* the principle of accountability and transparency. Nonetheless, the notion of accountability outlined in the GDPR is sensitively different from the administrative law one that has been outlined above. Conversely, the principle of transparency shares some interesting common features with the administrative law principle.

In the GDPR, accountability has become a central principle governing machine-driven data processing operations. In respect to the administrative law notion, accountability is only indirectly related to the purpose of participation and empowerment. To the contrary, it is related to data controllers' and processors' 'responsabilization' and is primarily linked to the object of verifiability, which is, in turn, related to risk management concerns. The GDPR expressly affirms that the principle of accountability under data protection law serves the function of detecting- and thus of signaling- whether an occurred personal data breach "is likely to result in a risk to the rights and freedoms of natural persons".

The accountability principle is established under art. 5.2 GDPR, affirming that 'the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability)'. By stating so, art. 5.2 GDPR establishes the autonomy of the principle of accountability in the data protection law ecosystem, and at the same time the strict operational connection to other principles relating to the processing of personal data- such as the principle of lawfulness, fairness, purpose limitation, data minimisation and ultimately of transparency.

As the same wording of art. 5.1 GDPR clarifies, the accountability parameter demands that compliance to normative requirements is externally verifiable, thus traceable. For these purposes, the principle of accountability is substantiated in the rules entailed in art. 22 GDPR, establishing that i) "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly

592 Other regulatory differences relate to enforcement and specifically relate to the exemption under art. 41.6 GDPR from the monitoring of approved codes of conduct with regards to the processing carried out by public authorities and bodies and the unavailability established under art. 79.2 GDPR of the option of bringing proceedings "before the courts of the Member State where the data subject has his or her habitual residence", in case the controller or processor is a public authority of a Member State in the exercise of its public powers".

593 O. Butler, *Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide,* cit. p. 560 ff..

affects him or her"; ii) "the right to obtain human intervention on the part of the controller"; iii) the right "to express his or her point of view and to contest the decision"; in art. 13.2 lett. f GDPR and art. 14.2 lett. g GDPR, requiring the controller to inform the data subject about "the existence of automated decision-making, including profiling (…) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (so-called 'right to explanation'); and ultimately in art. 58.1 lett. b GDPR that assigns to supervisory authorities the power to carry out "investigations in the form of data protection audits".

These measures strengthen the accountability regime of the GDPR respectively assuring a direct interaction between data subjects and data controllers (art. 22 GDPR); the release of information regarding the ratio and the legal effects of the data processing operations (art. 13.2 lett.f; art. 14.2 lett.g GDPR); the enactment of control mechanisms capable of signalling irregularities or system weaknesses in the management of personal data (art. 58.1 lett.b GDPR). All these measures encumber data controllers and processors with disclosure obligations that render processing activities transparent and thus traceable. In these regards, also in data protection law, transparency is a fundamental means to achieve accountability and is thus to be considered a key component of it[594].

As the same GDPR states, transparency "requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used (…)"[595]. More precisely, transparency "requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used"[596].

As in the context of administrative law, also in the data protection law ecosystem, transparency is primarily achieved through the right of access, which is established under art. 15 GDPR.

With regards to the content of the right to access, art. 15 GDPR provides a specific list of the information that needs to be made available to the data subjects. First of all, data subjects shall have the right to "obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to personal data"[597]. In addition to this, the right to access encompasses a variety of other types of information regarding, amongst others, "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject"[598]. The provision of "meaningful information about the logic involved" as well as of "the significance and the envisaged consequences of such processing for the data subject" concretises what has been

594 B Goodman, *A Step towards accountable algorithms?: Algorithmic Discrimination and the European General Data Protectio*n, 29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain, online available at http://www.mlandthelaw.org/papers/goodman1.pdf, p.7-9.
595 Recital 39 GDPR.
596 Recital 58 GDPR.
597 Art. 15 GDPR.
598 *Ibid*..

appointed as "the right to explanation"[599]. As some strand of the literature[600] has suggested, the expression "meaningful information" is to be interpreted as "legibility" of "architecture" and "implementation" of algorithmic processing[601]. Overall, it can be said that meaningful information about the logic involved must provide clarity with regards to the causal connections and the inference processes that orient the data-driven system so that the data subject may evaluate what type of consequences arise from the processing and thus exploit the remedies needed to address such "envisaged consequences". In this light, the proposed concept of "legibility" of the information to be provided under art. 15.1 lett. h GDPR is systematically consistent with the call for accessibility and understandability of the information regarding the processing entailed in the above-recalled recitals[602].

The right to access under art. 15 GDPR with its related transparency and explanation functions enables data subjects to verify the processing entities' conducts and more specifically their compliance with the data protection rules established by the Regulation. In this perspective, it is a primary tool for responsabilizing processing businesses and thus for achieving their accountability as defined in art. 5.2 GDPR.

Finally, it needs to be clarified that the effectiveness of the so-defined right to access is not destined to be blurred by the statements under recital 63 GDPR, affirming that the right to access "should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software". Although the balancing between individuals' right to data protection and businesses' intellectual property rights is debated in the literature[603], some strand of the scholarship[604] has convincingly argued in favour of the prevalence of the right to access over the protection of intellectual property rights, observing- amongst others- that the same recital 63 GDPR specifies that "the result of those considerations should not be a refusal to provide all information to the data subject", suggesting in this way that the right to access can be limited but never totally rejected.

As interpreted in these terms, the transparency rules entailed in the GDPR turn out to be precious regulatory tools for the networked algorithm-driven public decision-making, shedding light over the first stage of the complex public decision-making chain, that is the stage of the algorithmic processing carried out by private corporations. Since the outcomes of such processing activities come to define the courses of public decision making, the information provided on the basis of the mentioned GDPR's provisions to data subjects, become a useful means to empower citizens in respect to automated public adjudications and to control public interventions. The acknowledgment of the complexity of the "algorithmised" public administration decision-making

599 See, generally, M. Kaminski, *The Right to Explanation, Explained*, University of Colorado Law Legal Studies Research Paper, 18-24, 15th June 2018, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985, *passim*.

600 G. Comandè-G. Malgieri, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *IDPL*, 2017, 7, 4, p. 243-244.

601 *Ibid*..

602 Recitals 39 and 58 GDPR.

603 S. Wachter, B. Mittlestandt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation*, in *IDPL*, 2017, 7, 2, p. 76.

604 G. Comandè, G. Malgieri, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation,* cit. p. 263-264.

courses and of the structural and functional features of the new data protection law tools offered by the GDPR, thus ultimately reveals the significance of these same tools for public accountability purposes. With private parties assuming an increasingly important role in the performance of public functions through the grant of technological support, technical verifiability becomes an important source of political accountability.

5. The above-outlined analysis leads to two final considerations, one of practical and the other of more theoretical nature.

From a practical standpoint, the study has demonstrated that the increase in the private-public partnerships for the delivery of public services through algorithmic models, sensitively challenges the effectiveness of traditional administrative law tools of accountability and transparency of administrative decision-making. The unsuitability of traditional administrative law tools is mainly given by the fact that they cannot be applied to private processing entities and that public authorities cannot themselves access the relevant information concerning the algorithmic models employed for their decision-making since these are protected by strong intellectual property safeguards. In this light, transparency provisions entailed in the GDPR, and especially the right to access under art. 15 GDPR, assure the release of information regarding the privately conducted processing activities that increasingly orient public interventions. In this perspective, they become thus essential tools for data subjects to trace complex public decision-making courses and thus indirectly enhance political accountability as promoted by traditional access to public documents channels.

Against this backdrop, it appears that an integrated approach between new data protection law tools and traditional administrative law tools is needed in order to achieve a satisfying level of political accountability in respect to "algorithmised" public interventions. Such integrated approach is ultimately deemed to be essential for an effective protection of citizens' legitimate interests and fundamental rights that a short-sighted conception of public accountability would undermine in the shadow of algorithm-driven administrative rulings.

Ultimately, at a deeper level, the traced analysis reveals the complexity of the private-public divide in the algorithmic economy, requiring a rethinking of the interaction between different regulatory branches of European law and more precisely between different regulatory tools provided by these. The increasing intertwining between private and public parties for the algorithm-driven delivery of public services raises profound questions regarding the ways of integrating administrative and data protection law, the opportunity and limits of the applicability of general data protection law to public actors' processing activities as well as the functions to be assigned to traditional administrative law tools in the algorithmic environment[605].

GIULIA SCHNEIDER

605 In these regards, it is interesting to recall that the Administrative Tribunal of Lazio with the ruling has granted access to the information regarding the algorithms of a software employed by the Italian Public Administration for the purposes of the transfer of teachers under the Italian law 10/2015 under the right to access to public documents as established by art. 22 of the Italian law n.241/1990. So TAR Lazio-Roma, Sez. III bis, ruling 22 March 2017 n. 3769. For a comment see M. Iaselli, *Diritto di accesso all'algoritmo, TAR Lazio apre nuovi scenari*, published on the 17th May 2017, online available at http://www.altalex.com/documents/news/2017/05/17/diritto-di-accesso-algoritmo.

III.3

Artificial Intelligence in the public sector: opportunities and challenges*

SUMMARY: 1. Introduction. - 2. Public bodies and artificial intelligence: new opportunities by data-driven regulation. - 2.1. From data to granular knowledge. - 2.2. New ways of delivering public services. - 3. Automated decision-making: challenges for administrative law principle. - 3.1. A brief overview on the functioning of Artificial intelligence. - 3.2. GDPR protection: a "human-on-the-loop" meaning. - 4. Conclusion.

1. Nowadays, the most important challenge that public administration has to deal with is the management of a large amount of data.

At the beginning of the '90's, the process of digitalization has started, hence public administration begun to collect manually data related to administrative documents and procedures. The amount of data was insignificant, because of the traditional tools used to collect data and the shortage of digital resources[606]; but the trend changed when fast development of cloud computing and information and communication technologies (ICT) made it easier to generate, storage and analyse data.

It is true that public bodies are changing under legislative efforts, such as, firstly, Digital Administration Code (*d.lgs*. 82/2005) in order to digitalise own processes and organizations, in line with administrative principles.

The digitalization process provide a «logical data»[607] structure instead of a «logical documents» one, with the consequence that artificial intelligence's outcomes as well as data derive from digital sources (*i.e*. database interconnected, public platform) should be introduced in the procedure under the public bodies' control.

The shifting to logical data paradigm makes the phase of managing and collecting data crucial for the legality of proceeding. Therefore, artificial intelligence's outcomes could be considered «legally relevant»[608] as long as they are generated under a legal framework.

Consequently, one of the main revolution that public bodies have been living is the shifting from digitalization to datafication[609] that is an approach that considers that all elements could be quantified and analysed. This phenomenon is due to information technologies available at lower cost and their ubiquity throughout society.

606 * Paper reviewed and updated, presented during the Seminar on "*Big Data and Public Law: New Challenges beyond Data Protection*", Gargnano sul Garda, 15-17 October 2018.

On the contrary, nowadays documents are borm digital and data can be collected immediately.

607 See E. MENICHETTI, *Accessibilità e tutela della riservatezza*, in B. PONTI (a cura di), *Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale,* Santarcangelo di Romagna, 2008, pp. 181 ss.

608 The article 1, *comma* 1, *lett*. p) of Digital Administration Code (*d.lgs*. 82/2005) considers «informatic document all document in which there is the digital representation of acts, facts and data legally relevant».

609 V. MAYER-SCHONBERGER AND K. CUKIER, *Big data*. *Una rivoluzione che transformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013, pp. 103 ss. created the term *datafication* and give some examples of ubiquity of ICT and the possibility of quantify everything, such as location, relations, own self, words, and so on.

III.3

Due to advanced ICT tools, public and private actors collect and analyse an impressive quantity of data.[610] Related to public sector, this revolution influence policy and rulemaking process because predictive analytics on ICT's outcome could facilitate the merging of scattered data and the establishing of unexpected correlations.

Internet of things throughout the city, social networks, digital procedures, e-mails and so on are just some of the instruments, which public bodies and people use every day to produce and capture a significant amount of data.

Everywhere there are data, thus the ability of collecting and analysing them is crucial «to do more, better, faster and more cheaply»[611]: public bodies have to understand this improvement urgently and to govern it, both in order to re-think how public services could be delivered and to preserve administrative principles into administrative proceedings.

It is clear that this huge amount of data poses both opportunities and challenges to the administrative law system, which scholars have to face[612].

On the one hand, big data and artificial intelligence create new opportunities to understand reality in a deep way, thanks to specific tools (such as Internet of Things, predictive analysis and datasets) and new ways of working (*i.e*. interoperability and sharing between public bodies) and new ways of government (i.e. data driven regulation).

On the other hand, however, they pose some questions, related to administrative principles, especially to due process, rule of law and accountability.

In this way, General Data Protection Regulation 2016/679 (GDPR) represents the first attempt to unify the fundamental right of data protection and, at the same time, the free circulation of data in a safe and trustworthy digital society. In particular, one of the main purpose of GDPR is to protect rights and freedoms of people as a whole and not only the ones of data subjects.

For this reason, scholars may appreciate both the public aim of this act and the attempt of regulating the rise of artificial intelligence in the public sector to protect rights and freedoms.[613] Starting from these characteristics, this contribution would offer some insights in order to re-think and to adapt traditional legal categories and principles, i.e. due process, to this new phenomenon.[614]

GDPR tries to highlight the central role of guide-principles, such as accountability and transparency and, at the same time, it provides for specific rights to recipients. It pays attention to

610 Public bodies collect a large amount of data during own activities, called administrative data; indeed private sector collect data, namely, from e-commerce, payment transaction, trade agreements and so on.

611 In this way, M. MACIEJEWSKY, *To do more, better, faster and more cheaply: using big data in public administration*, in *International Review of Administrative Sciences*, 83, 2017, pp. 120-135.

612 It is a matter of fact that the big data phenomenon has been studied under several point of views, such as technological, urban policy and protect of privacy ones, while only recently legal scholars have started to study it.

613 F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale,* in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 164 ss. The Author argues, «to the heart of GDPR there are people with their rights and freedoms», p. 165.

614 O. POLLICINO, *Tutela dei diritti fondamentali nell'era digitale e contest valoriale: una indagine transatlantica*, in *Rivista di diritto dei media*, 2, 2018, suggests that changes of digital area push scholars and judges towards two ways. They could choose to transfer *sic et simpliciter* traditional legal categories into digital scenario or they could choose to re-think and adapt them to new scenario. This choice is hardly influenced by cultural framework (resistance to or openness to the innovation).

these aspects with the aim of significantly enhancing people's trust about the use of new methodologies in the public decision-making, such as big data analytics, internet of things and artificial intelligence, with the final purpose of protecting people affected by.

Artificial intelligence uses as main raw material a huge amount of data (also known as big data), with the consequence that accessibility and correctness of data are a pre-condition to guarantee a good administration principle and to protect rights and freedoms. GDPR focuses on these elements in order to be both a normative framework to avoid pervasive as well as unreasonable public control and a tool for improving a sound data circulation.

Scholars must urgently assess what are the consequences of the administrative decision-making process in the machine-learning era. In particular, attention should be paid to two issues: data quality and compatibility between artificial intelligence and well-established administrative principles.

Consequently, the quality of data, collected and used for decision-making process, is one of the main challenges that public administration has to deal with.

Strictly connected to the first one, the second challenge is about the consideration of legal compatibility of automated individual decision making with principles of administrative law. Scholars should have the ability to re-address this new kind of activities into the legal framework, using renewed and adapted old traditional categories to the concerns connected to the machine-learning era[615].

However, artificial intelligence could strengthen regulatory public administrations to make them smarter or able to develop data-driven regulation, so that they permit to turn good administration principles into reality. Hence, scholars may be optimistic about artificial intelligence used by public administrations, but, for doing that, the re-thinking of traditional guarantees must be a priority.

Article 22nd GDPR expresses that data subject have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him/her or similarly significantly affects him/her. Nevertheless, GDPR permits automated processing even if there are some legal guarantees, such as the right to obtain human intervention, the right to be heard and the right to contest the decision.

In a literal interpretation, GDPR offers some tools to allow public administrations to use artificial intelligence legally, namely in a way that permits them to be transparent and to act reason-giving in order to preserve due process principle. In particular, scholars could individualize ways to standardize rights and procedure to concrete them, to well-defining *ex ante* duties on civil servants, artificial intelligence and programmers and to make the functioning of artificial intelligence transparent.

In order to enhance public accountability and transparency, algorithmic impact assessments may be introduced in the public-sector procedures to correct bias and to augment protection (for example, discrimination could be prevented).

615 About the inadequacy of old categories to the digital era, see L. FLORIDI, *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, 31, I, pp. 1-8 available at https://link.springer.com/article/10.1007%2Fs13347-018-0303-9.

To sum up, in the second chapter of the article I try to highlight how artificial intelligence redefines the way of delivering public services; in particular the rise of evidence-based methods could change administrative decision-making process (*i.e.* data driven regulation) and, more generally, boundaries of public function.[616]

In the third chapter, I pay attention to challenges, which public bodies deal with, relating to the introduction of artificial intelligence in an adjudicatory proceeding. The main challenge is about automated decision-making, consequently I suggest a "human- on-the-loop" interpretation of article 22nd GDPR in order to preserve administrative principle and to avoid discriminations. Moreover, I prompt an extensive interpretation of good administration principle in order to preserve accountability.

Scholars should reflect about these opportunities and challenges both to overcome oppositions against the introduction of artificial intelligence in the public sector and to shape a new cultural framework based on renewed and adapted legal categories to the new digital context in order to guarantee procedural and jurisdictional rights and freedoms' protection.

2. A big amount of data is useful to public administration for at least two reasons: both the better government of the city and the completeness of inquiry activities during the administrative procedure.

My focus will be just about the first point on data collected for issuing administrative decisions: this new kind of regulation calls data-driven regulation.

In the ICT era, data science and big data allow public administrations to analyse, store and process a large amounts of collected data in order to take administrative decisions, plans, strategies and actions better fit to citizens' needs[617]. It is important to underline that «the usefulness of big data is followed by multiple levels of operational steps, such as acquisition, information extraction and cleaning, data integration, modelling and analysis, and interpretation and deployment».[618]

The main revolution of this age is the possibility for public administrations to collect a large amount of personal data on citizens and daily commuters or tourists, known as administrative data[619] as well as urban data on city infrastructures and utilities (such as traffic, public transports

616 It is particularly interesting the study of G. CARULLO, *Gestione, fruizione e diffusion dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2018 in which he highlights how ICT could change the way of public bodies' working and the relationship with citizens. Especially, under the ICT push, participatory rights, transparency, regulation and public service delivering, as I try to explain below in chapter 2.2. Another point of view is also offered by S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione dell'amministrazione,* in D. SORACE, L. FERRARA, S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *A 150 anni dall'unificazione amministrativa italiana. La tecnificazione*, IV, Firenze, 2017 in which the relation between digitalization, public administration and citizenship is deeply analyzed.

617 About the possibility to re-design the delivery of services, see F. MALOMO and V. SENA, *Data intelligence for local government? Assessing the benefits and barriers to use of big data in the public sector,* in *Policy and Internet,* 9, I, 2017, pp. 7-27.

618 S. K. PAL, S. K. MEHER, A. SKOWRON, *Data science, big data and granular mining*, editorial in *Pattern Recognition Letters* 67, 2015, pp. 109–112.

619 Administrative data derive from the operation of administrative systems, as information collected for the purposes of registration, transaction and record keeping. Frequently, administrative data derived from a wide range of administrative systems such as those in education, healthcare, taxation, housing or vehicle licensing as well as registers of births, deaths, marriage and so on. See R. CONNELLY, C. J. PLAYFORD, V. GAYLE AND C. DIBBEN, *The role of*

routes, number of services access). It represents a unique opportunity to inform policy and regulation for governing the growing problems of unsustainable urban expansions, inequality and insecurity and other governance problems. In this way, the employment of data science, big data, Internet of things, algorithms and predictive analytics are useful to enhance efficiency of their services and decision-making.[620]

2.1. Throughout the centuries, public bodies collected data about cities and their citizens in a very large datasets based on relatively limited samples, in a specific time and space, with the restricted number of variables. They have been defined as small data, which are referred to data captured with questionnaire surveys, case studies, city audits, interviews and focus groups as well as national censuses[621], and government records. Limited and out of time are characteristics of small data because of inadequate tools for capturing and analysing them and, consequently, scholars and researchers undertook to limit the collecting of data[622].

Something changed when statistics demonstrated that casualty makes samples better[623] and when new powerful information and communication technologies have been developing and employed: the data revolution era begins.[624] In fact, not only the possibility to collect and store data, but also the possibility to interconnect[625] and mash data gathered by different institutions represent

administrative data in the big data revolution in social science research, in *Social Science Research,* 59, 2016, particularly p. 3.

620 Firstly, Michael Abramowicz, an American economist, argued that predictive analysis is useful in the market regulation, because it is possible to predict more effectively the outcome on cost-benefit, see M. ABRAMOWICZ, *Information Markets, Administrative Decision-making, and Predictive Cost-Benefit Analysis*, in University of Chicago Law Review, 71, 2004. See also J. MITTS, *Predictive regulation*, June 27, 2014, available at SSRN: https://ssrn.com/abstract=2411816 or http://dx.doi.org/10.2139/ssrn.2411816, who considers predictive analysis to better individualize regulatory priorities.

621 For example, Catholic churches developed databases on birth and death of people or their marriage; municipalities used tools for processing census information.

622 Some authors consider it as an artificial line due to the inadequacy of tools; see V. MAYER-SCHONBERGER AND K. CUKIER, *Big data. Una rivoluzione che transformer il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013, pp. 34 ss.

623 This assumption is considered important to shift from causation rules to correlations one, that is the Big data's method of research.

624 A new paradigm arises, from one in which it was important to manage and control a little amount of data to another in which it is important to manage and collect as data as possible; see M. FALCONE, *Le potenzialità conoscitive dei dati amministrativi nell'era della "rivoluzione dei dati": il caso delle politiche di eradicazione dell'epatite C,* in *Istituzioni del federalismo,* 2, 2017, p. 426.

625 At the beginning of 90's when the digitalization of Italian public administration was at dawn, A. MASUCCI, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione,* Napoli, 1993, p. 67 wrote that the rationality parameter, which informs administrative proceedings, impose «the necessity of connecting different public bodies in order to share data storage everywhere». See also, G. CARULLO, *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse*, in C*oncorrenza e mercato*, 23, 2015.

one of the main revolution[626] for public bodies in the digital era that allows public bodies to have a granular[627] and deeper knowledge about society.

Data refers to «units or morsels of information that as a whole form the bedrock of modern policy decisions by government and nongovernment authorities», so data is the «starting point for what we know»[628], especially if data represents almost all pieces of information available.[629]

Informational and communicational technologies provide «a deeper, more holistic and robust analysis»[630] because of the indexical objects, which are embedded into almost all urban and environmental spaces as well as able to communicate and share data among each other, in order to obtain new derived data.

For example, throughout the city there are a network of cameras and transponders for capturing data, which feed back to a central control hub, where analysts could monitor the flow of traffic and could modify traffic light sequences and speed limits as well as automatically punish traffic violations.[631]

Basically, public and private actors create a citywide instrumented system that unify together data streams from different agencies related to different public services into an hub service centre.[632] Here, these data are visualized and monitored by analysts' process, which could aggregate data over time and huge volumes of administrative data. After these operations, these correlations appear on a virtual operations platform that enables city officials to have significant information on different flows throughout the city.

In this context, data science, big data and other technologies have an important role in the enhancing of public powers because they facilitate both the collection of data, and the interconnection among several public administration databases[633] and they allow public bodies to convert scattered data into valuable knowledge. Therefore, «governments are central to both

626 Just at the beginning of the 2000's, some scholars considered that telematics was a good opportunity for public administrations to innovate and became transparent and more efficient them and to make simpler relationship between public bodies and citizens. See P. MERCATALI, *Informatica applicate alla pubblica amministrazione,* Simone, 2003.

627 As an example of some doctrine, R. KITCHIN, *The real-time city? Big data and smart urbanism*, in *Geo Journal*, 79, 2014, p. 2; S. ALLWINKLE AND P. CRUICKSHANK, *Creating smarter cities: an overview*, in *Journal of Urban Technology*, 18, 2011, p. 2; S. K. PAL, S. K. MEHER, A. SKOWRON*, Data science, big data and granular mining*, in *Journal Pattern Recognition Letters*, 67, 2015, p. 110, in which they consider how granular mining permits to understand society meticulously.

628 S. RANCHORDAS AND A. KLOP, *Data-driven regulation and governance in smart cities*, in *Handbook on Data Science and Law,* A. BERLEE, V. MAK, E. TJONG TJIN TAI, Edward Elgar, 2018, p. 8.

629 Some case studies conducted by ALBERT LASZLO-BARABASI permit to understand how a complex system works: it is possible thanks to a huge amount of data collected and analysed useful to highlight something new and previously unknowable.

630 R. KITCHIN, *The real-time city? Big data and smart urbanism,* in *Geo Journal*, Springer, Dordrecht, 79, 2014, p. 7.

631 Many other examples are possible: smart tickets could trace passenger travel; transponders could measure vehicle flow or empty spaces in a car park; SEE R. KITCHIN, *The real-time city? Big data and smart urbanism*, cit.; R. KITCHIN, T. P. LAURIAULT AND G. MCARDLE, *Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards,* in *Regional Studies, Regional Science,* 2015.

632 One of the main specialized examples in Italy is Consorzio per il Sistema Informativo – CSI, which makes big data analysis in Piedmont.

633 This activity is technically called massive data integration.

creating and managing knowledge»[634] because they do not just produce knowledge, but also manage it, especially with the aim of «serving the public interest».[635]

On the one hand, it is clear that ICT offer the possibility to see an objectively measured, well defined as well as a real-time analysis of everyday life, infrastructures and needs, consequently public bodies could use these significant information and try to regulate the services of the city and to offer public services more focus-oriented.

On the other hand, predictive analytics permit to establish new correlations between pieces of information: this method of knowledge overturns the traditional way, based on causation rules.

Thanks to Big data analytics, public bodies have the ability to find useful correlations within datasets «without understanding causation»[636]; nonetheless, it is important that users have in mind that there is «the risk of finding spurious correlations».[637] Anyway, with improved statistical and computational methods and the possibility of linking different datasets could begin a new process of creating knowledge. In particular, the big data revolutions is based on patterns, which come from linkage and connections about pieces of data, which the ordinary human assessment could not understand.[638]

It is also useful to highlight that these data offer knowable and governable systems, which show a rational, mechanical, linear and hierarchical ways of being.[639] This knowledge is useful for public bodies in order to act effectively and efficiently. In fact, they could see «the world as it actually is through descriptive statistics and visual representations»[640]. The use of indicator,

634 C. FREDRIKSSON, F. MUBARAK, M. TUOHIMAA AND M. ZHAN, *Big data in the public sector: a systematic literature review*, Scandinavian Journal of Public Administration, 21, III, 2017, p. 47.

635 H. MAUREEN, *The value and challenges of public sector information,* in *Cosmopolitan Civil Societies: an interdisciplinary approach,* 5, III, 2013, p. 81.

636 J. SHAW, *Why big data is a big deal*, in Harward Magazine, 116, IV, 2014, p. 33. H. EKBIA, M. MATTIOLI, I. KOUPER, G. ARAVE, A. GHAZINEJAD, T. BOWMAN, V. RATANDEEP SURI, A. TSOU, S. WEINGART, C. R. SUGIMOTO, *Big data, bigger dilemmas: a critical review,* in *Journal of the association for information science and technology*, 66, VIII, 2015, p. 1529 ss. pay attention to the historical evolution about the epistemological paradigm and they argue that «the distinction between causal relation and correlation is at the center of current debates…..a debate that has been going on for decades,..between the advocates of data-driven science and those of theory-driven science». Also J. COWLS AND R. SCHROEDER, *Causation, correlation and Big Data in social science research,* in *Policy & Internet,* 7, IV, 2015, pp. 447 ss. show debate about methodological change, from causation paradigm to correlation one and the consequence about social science research.

637 J. SHAW, *cit.*, p. 34.

638 In addition, M. FALCONE argues that big data analytics are deeply changing the way in which public bodies know; see M. FALCONE, *Le potenzialità conoscitive dei dati amministrativi nell'era della "rivoluzione dei dati"*, cit., pp. 423 ss. An interesting point of view is offered by H. EKBIA, M. MATTIOLI, I. KOUPER, G. ARAVE, A. GHAZINEJAD, T. BOWMAN, V. RATANDEEP SURI, A. TSOU, S. WEINGART, C. R. SUGIMOTO, *Big data, bigger dilemmas: a critical review,* cit., p. 1527; in this article they consider that, in a cognition-oriented perspective, the limited capacity of the human mind to make sense of large amounts of data requires «mediation through trans-disciplinary work, technological infrastructure, statistical analyses, and visualization techniques to enhance interpretability».

639 Study on network science, system complex and self-organization principle of system complex show that «our action are led by rules, schemes and mechanisms», consequently there are reproducibility and predictive ability as in hard science, A. LASLO-BARABASI, *Lampi. La trama nascosta che guida la nostra vita,* Torino, 2011, p. 13; see also R. CAVALLO PERIN, *Beyond the municipality: the city, its rights and its rites,* in *Italian Journal of Public Law,* 2, 2013, pp. 307-315.

640 F. ASTLEITHNER AND A. HAMEDINGER, *The analysis of sustainability indicators as socially constructed policy instruments: benefits and challenges of "interactive research",* in *Local Environment*, 8, VI, 2003, pp. 627-640.

benchmarking and dashboard, as well as big data analysis and internet of things permit to capture the external reality in a fully and representative way.

Some authors[641] consider data as value-free and objective tools of knowing the city, based on the assumption that data are independent of ideas and contexts. In this sense, data are simply able to reflect the truth without subjective interpretation.

Indeed other authors[642] are critical because of the assumption that data do not exist independently of the ideas and of instruments used to generate process and analyse them. In fact, data «is the product of choices and constraints, shaped by a system of thought, technical know-how, public and political opinion, ethical considerations, the regulatory environment and funding and resourcing…framed and used contextually to try and achieve certain aims and goals»[643].
This latter interpretation is partially true and it is a relevant challenge that public bodies deal with. In chapter 3, I develop this idea because I am critical about algorithmic functioning in relation with legal categories and principles.

Anyway, the outcome knowledge represents the substance of data-driven regulation and thanks to this, public bodies could issue administrative decisions, plans, strategies and actions for better managing infrastructures, for allocating urban resources and for nudging citizen, tourist and daily commuters in order to govern the city in an efficient way.

Consequently, it seems proper to consider that the delivering of public services are changing deeply, from a traditional way to an innovative one.

2.2. In the Italian administrative system, the delivering of public services is based on authoritative and unilateral decision, as a result of the application of rational rules.
In fact, the Italian Constitution establishes at the article 41 that public or private actors must deliver public services according to the law that orders plans and controls, which actors must operate to reach social objectives.

It seems interesting to analyse how big data, artificial intelligence and predictive tools could transform the way of planning and controlling public services.

First, it appears that the law is not the only way to better individualize citizens' needs and, secondly, it seems partly outdated to consider that only the law, as stated by the Constitutional Court[644], individualizes social purposes.

641 D. ROSENBERG, *Data before the fact*, in L. GITELMAN, *Raw data is an oxymoron,* Cambridge, MIT press, 2013, pp. 15-40.

642 T. P. LAURIALT, *Data infrastructures and geographical imaginations: Mapping data access discourses in Canada,* Phd thesis, Carleton University, Ottawa, 2012, available at https://curve.carleton.ca/system/files/etd/7eb756c8-3ceb-4929-8220-3b20cf3242cb/etd_pdf/79f3425e913cc42aba9aa2b9094a9a53/lauriault-datainfrastructuresandgeographicalimaginations.pdf; G. BOWKER AND L. STAR, *Sorting things out: classification and its consequences*, Cambridge, MA: MIT press, 1999; R. KITCHIN AND M. DODGE, *Code/Space: software and everyday life*, Cambridge, MA, MIT press, 2011; R. KITCHIN, *The data revolution: Big data, open data, data infrastructures and their consequences*, Sage, London, 2014; D. RIBES AND S.J. JACKSON, *Data bite man: the work of sustaining long-term study,* in L. GITELMAN, *Raw data is an oxymoron,* Cambridge, MIT press, 2013, pp. 15-40.

643 R. KITCHIN, *The real-time city? Big data and smart urbanism*, cit., p. 9.

644 The reference is to judgement n. 29/1957, in which the Italian Constitutional Court established that social purposes were individualize by «general and social needs, determined by the law».

These assumptions are overcome by the fact that citizens' needs are individualized with sensors networks[645] (such as cameras, light monitors, proximity sensors), cloud computing and digital platforms.

As mentioned above, with big data analytics public bodies could analyse behaviour of public services' users in real-time, predict their needs and respond to potential crisis in a very short-term.

It is noteworthy to consider that the use of predictive tools, artificial intelligence and big data allow public bodies to overcome traditional procedures of law making based on «anecdote or intuition or clientelist politics or periodic/partial evidence»[646] and «paternalism»[647].

Hence, these tools permit to shift «from fact-free policy to rational and evidence-based rules»[648]; in particular, some case-studies[649] demonstrate that informational technology architecture, predictive analytics algorithm and data governance «define a mechanism for transforming from a reactive mode of operation based on gut instincts to a proactive mode of operation based on mathematical models»[650].

A proactive approach is based on tools, which are able primarily to identify indicators and to collect insights (*i.e.* data); secondly, to integrate, unify and analyse data from different sources in order to develop a predictive, flexible model useful for giving relevant information. The result

645 This expression refers to very small sensors or actuators embedded or placed on different structures to measure specific predefined outputs, such as movement and speed of traffic jam, levels of light, temperature and air pollution.

646 R. KITCHIN, *The real-time city? Big data and smart urbanism*, cit., p. 7.

647 F. DI PORTO AND N. RANGONE, *Cognitive-based regulation: new challenges for regulators?*, in *Federalismi. Rivista di dirittopubblicoitaliano, comunitario e comparato*, 20, 2013, p. 7, in which Authors argue that nowadays public bodies and other regulators could overcome the lack of knowledge about real people, consequently traditional regulatory strategies based on paternalistic objectives seem to be enriched with crucial information in order to be more focus-oriented.

648 S. RANCHORDAS AND A. KLOP, *Data-driven regulation and governance in smart cities*, cit., p. 12. About the rising of evidence-based law making, see R. VAN GESTEL AND J. DE POORTER, *Putting evidence-based law making to the test: judicial review of legislative rationality*, in *The theory and practice of legislation*, 4, 2016, pp. 155-185. Authors analyse how this kind of law making process is rising with the consequence of shifting from codification of existing customs to modification of human behaviour. In particular, the article's core is how courts could judge about legislation and regulation based on evidence fact and scientific researches. It might consider that subsidiarity and proportionality play an important role to conduct procedural review. Proportionality as external or internal limits to the use of big data insights as well as cognitive ones in regulation. Proportionality must lead public bodies' choices with or without artificial intelligence; but, especially, in public sector the use of ICT should be less intrusive as possible because of the leading of public interest. For wider examination see R. ANGELINI, *Intelligenza artificiale e governance. Alcune riflessioni di sistema,* in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 298 ss.

In other fields of knowledge, such as economics, scholars pay attention to the overcoming of paradigm of rational choice in favour of cognitive-based one. This shifting is important because of the unprecedented attention to real people, their behaviours and habits in order to analyse people's decision-making mechanism. This awareness allows public bodies (and other regulators in general) to make «better formulation of rules and the provision of more adequate responses to the public interest they are intended to satisfy», see F. DI PORTO AND N. RANGONE, *Cognitive-based regulation: new challenges for regulators?*, cit., p. 3

649 An example of case study is conducted by an IBM RESEARCH TEAM on property vacancy problem in Syracuse city, NY in 2011, as a result of IBM's Smarter Cities Challenge project (www.smartercitieschallenge.org).

650 S. APPEL ET AL., *Predictive analytics can facilitate proactive property vacancy* in *Technological forecasting and social change,* 89, 2014, p. 172.

represents the «core information that can be used to make policy decisions, understand gaps and monitor the status of actions and their impact on achieving the desired outcomes».[651]

Some literature show that the activity of planning public services is shifting from a predetermined and authoritative activity to a predictive and proactive one: in this way, policy development is based on a comprehensive view of the city and it allows public bodies to act more focus-oriented and to reshape local services. In the digital age, nodality is one of the four properties[652] that public bodies should have for pursuing effective objectives: that is, public bodies should put themselves «in the middle of an information»[653] because of their «social centrality and visibility»[654]. Thanks to their own strategic position as nodal receivers public bodies could receive and give information in order to better govern.[655]

Public bodies could have some benefits from this way of knowing needs, because they could issue regulatory acts efficiently, forecast risks and prevent restrictions on competition[656]: they could use information as object as well as tools of regulation.

Evidence-based method is based on deeply knowledge of trends and on *ex ante* perspective, hence on knowledge available at the time of regulation: evidence-based law-making process is not new, but it is growing thanks to indicators suites, which capture real-time data and represent them on dashboard graphs, which provide detailed information about city performance. Nowadays, this kind of process has been pushed by powerful technologies[657] and «the desire to reform the public sector management of city services to make them more efficient, effective, transparent and value for money, combined with citizen and funder demands»[658].

3. In the public sector, the use of big data analysis, predictive analysis, internet of things and so on, creates some concerns.

651 S. APPEL ET AL., *Predictive analytics can facilitate proactive property vacancy*, cit., p. 167.

652 C. HOOD AND H. MARGETTS in *The tools of government in the digital age,* Palgrave, 2007 individualize four properties useful for a government in the digital era: nodality, authority, treasure and organization. Governments should be in the middle of information and have a legal or official power, as well as money or anything which could be freely exchanged and people with specific skills.

653 C. HOOD AND H. MARGETTS, cit., p. 5.

654 C. HOOD AND H. MARGETTS, cit., p. 8.

655 In the network science discipline nodality is crucial property. In fact, every complex system (social, biological, technological, trade, energy and so on) have a structure based on central node and link that connect each other. There are some huge node, called hub, which gather many nodes; consequently, hub becomes important for the stability of the system, see A. LASLO-BARABASI, *Network science,* Cambridge University Press, 2016, pp. 247 ss.

656 F. DI PORTO, *L'informazione come "oggetto" e come "strumento" di regolazione (il caso dei mercati energetici al dettaglio),* in *Riv. Trim. dir. Pubb.,* 4, 2011, pp. 975 ss., in which Author argues that information plays an important role for regulators in the information and communication technologies era. Author examines the role of information in the retail energy market and she takes into account the development of nudging and reflexive governance as two new ways of government.

657 It is necessary to underline that since the early 1990's some indicators (single and composite) have been used to capture details of city, but only with potential computational and mining process, data are very useful for public bodies.

658 R. KITCHIN, T. P. LAURIAULT AND G. MCARDLE, *Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards,* in *Regional Studies, Regional Science,* 2, I, 2015, p. 8.

The first reason is that public bodies and the government have always been considered «of the people, by the people».[659] Connecting to this idea, information and communication technologies should be subordinated to humans.

The second reason regards the respect of rule of law and the achievement of public interest. Undoubtedly, public bodies benefit from the use of technological tools, but, as the public interest requires, they must respect administrative principles.

Many concerns about artificial intelligence rise from their ubiquity[660], their uncertainty about legitimacy and their hiddenness and opacity of functioning, based on algorithms[661].

Some studies[662] demonstrate that algorithmic perception changes relating to the nature of decision-maker as well as tasks, which they do. In particular, if artificial intelligence does mechanical tasks, people perceive them as equally fair and trustworthy because of their efficiency and objectivity; indeed, if artificial intelligence does human tasks, people perceive them as less fair and trustworthy because of their lack of intuition and their dehumanization.

Moreover, the use of artificial intelligence in the public sector poses some questions about legitimacy[663] because «algorithms structure and constrain the ways in which humans act»[664]; on one hand, legitimacy could exist in an instrumental way that is the better goals are gained, more legitimate they are. On the other hand, procedure could legitimate tools if they allow recipients to participate and contribute to decision-making.

The classification above permits to argue that in our administrative system we should prefer a mixed approach, in which public bodies preserve procedural rights as well as tools' efficiency, as I examine below in chapter 3.2.

In addition to these concerns, another one rises related to artificial intelligences' opacity. These tools rely on predictive or descriptive algorithmic processes that allow public bodies to discover useful patterns and outcomes as well as to take decisions. Concerns rise to unknowable and unpredictable data-mining proceedings not based on rationales and factors understandable by humans. This complexity of algorithmic proceeding creates some problems to the due process

659 C. COGLIANESE AND D. LEHR, *Regulating by robot: administrative decision-making in the machine-learning era,* Institute for law and economics, University of Pennsylvania Law School, research paper, 8, 2017, pp. 1152 ss.; they report a phrase of Abraham Lincoln's speech at Gettysburg Address on 19th of November 1863 available at http://rmc.library.cornell.edu/gettysburg/good_cause/transcript.htm.

660 In this article, I do not argue about concerns on surveillance and privacy issues.

661 Here, I adopt the algorithm definition elaborated by T. GILLESPIE, *The relevance of algorithms*, in *Media technologies: Essays on communication, materiality, and society,* T. GILLESPIE, P. J. BOCZKOWSKI and K. A. FOOT (eds.), Cambridge Mass., MIT Press, 2014, pp. 167; also N. DIAKOPOULOS, *Algorithmic Accountability*, in *Digital Journalism*, 3, III, 2015, 400.

662 M. K. LEE, *Understanding perception of algorithmic decisions: fairness, trust and emotion in response to algorithmic management*, in *Big data and society,* 2018, pp. 1-16; M.K. LEE AND S. BAYKAL, *Algorithmic mediation in group decisions: fairness perceptions of algorithmically mediated vs discussion-based social division*, in *CSCW '17 Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing,* pp.1035-1048.

663 As J. DANAHER argue, legitimacy is the property that coercive public decision-making processes must possess if they are to rightfully exercise the requisite authority over our lives; about the regulation of human behaviour by algorithms, see L. LESSIG, *Code: And other Laws of Cyberspace*, Basic Books, New York, 1999.

664 J. DANAHER, *The threat of algocracy: reality, resistance and accommodation,* in *Philosophy technology,* Springer, 2016, p. 3 .

principle because it should be preferable that decision-making procedures are rationally comprehensible to those who are affected by them[665].

Two solutions could be suggested in order to preserve due process principle in automated-decision making: to enhance participatory rights according to article 22nd of GDPR and to re-think good administration principle, applicable *ex ante.*

3.1. Artificial intelligence and algorithms are useful tools for making public bodies' operational activities faster and more efficient.

As mentioned above, artificial intelligence works with the use of machine learning techniques, which are able to learn on their own, starting from training and testing data. In particular, algorithms in machine learning change in response to their output and «automatically improve with experience».[666]

Basically, all data collected in ways mentioned above, are used by developers to programme machine learning tools. Consequently, these data are previously divided in testing and training data[667], then machine learning techniques use them in an unknowable way.

This property is called "black box"[668] and create some ethical and legal concerns that scholars have to face for preserving rights and freedoms as well as administrative law principles.

Especially, some concerns arise when artificial intelligence is used in an automated decision-making.

Machine learning techniques base on profiling activities, consequently, it is likely the risk of unjustly stereotyping individuals for their ethnicity, lifestyle or residence. Hence, the surveillance on data quality without discrimination biases is important duty on public bodies in order to preserve due process principles, and good administration.

In fact, algorithmic bias could contribute to the risk of stereotyping, especially if biases exist in the «data used to train deep learning systems»[669]. For example, public bodies could deliver, or

665 In this sense, also P. SAVONA, *Administrative decision-making after the Big data revolution*, in www.federalismi.it, 19, 2018. Similar problems could arise in criminal proceeding law, as evidenced by S. QUATTROCOLO and U. PAGALLO, *Fair trial and the Equality of arms in an algorithmic society*, in *Global Law. Legal answers for concrete challenges,* M. L. LABATE MANTOVANINI PADUA LIMA and J. GARCEZ GHIRARDI (eds.), 2018, pp. 261-274; S. QUATTROCOLO, *Equità del processo penale e automated evidence alla luce della Convenzione Europea dei Diritti dell'Uomo*, in *Revista Italo-Espanola de Derecho Procesal*, 2, 2018, reperibile al sito http://www.rivitsproc.eu/es/articulos/equita-del-processo-penale-e-automated-evidence-alla-luce-della-convenzione-europea-dei-diritti-delluomo/.

666 T. MITCHELL, *Machine learning*, Indian edition, 1997, p. XV.

667 Supervised machine learning is based on each data labels with its correct reference so that the algorithm knows when it is making errors. Unsupervised learning uses unlabeled data, so that performance criteria being optimized are not measures of error rates, because the truth is not known, but measures of similarity between digits determined by the algorithm to be the same. See C. COGLIANESE AND D. LEHR, *Regulating by robot: administrative decision-making in the machine-learning era*, Institute for law and economics, University of Pennsylvania Law School, research paper, 8, 2017, pp. 1158 ss.

668 F. PASQUALE, *The black box society. The secret algorithms that control money and information,* Harvard University Press, 2015, p. 3 in which the Author highlights that it is a useful metaphor that represents «a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other».

669 GOVERNMENT OFFICE FOR SCIENCE, *Artificial intelligence: opportunities and implications for the future of decision making*, 2016, p. 14.

not, some public services or other benefits because of historical data on individuals, that could be discriminatory and reflect, consciously or unconsciously, biases.

3.2. In order to avoid discrimination on public decisions, article 22nd of General Data Protection Regulation 2016/679 (GDPR) provides for some rights to recipients[670] and it bans all decisions that are adopted solely on automated processing, because of concerns mentioned above.

This article should require that public bodies must fully respect rights, such as to give specific information to data subjects, to guarantee the right to obtain human intervention, to express one's own point of view, to give a full reason giving and the possibility to challenge the decision.

In my view, this article provides a human-on-the-loop[671] perspective, that is, artificial intelligence could work autonomously, but the human oversight and override are guaranteed. In this case, civil servants could decide whether follow or not artificial intelligence's outcome[672].

In the digital era, new duties for public bodies rise[673]: on the one hand, they should control how developers produce algorithms. Indeed, algorithms are value-laden[674] and, in spite of their efficiency, they could reproduce discrimination biases.[675] For these reasons, public bodies should extend own control *ex ante*, especially during the programming phase.

In order to preserve good administration and impartiality, public bodies have to control how programmers and engineers programme algorithms as well as have to give specific duties to them[676]; for example, public bodies could cooperate with engineers to provide guidelines on legal framework and technological measures for compliance (*i.e*. legal by design).

I argue that the difference between private and public sector must be preserved: artificial intelligence, which is programmed for public bodies activities will be very different in scope and in way in which rights are protected.[677] Public bodies could provide compliance rules and principles to programmers in order to build artificial intelligence in line with administrative principles.

670 For a critical perspective about right to explanation (articles 13-15), see S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law,* 7, II, 2017, pp. 76-99, available at: https://academic.oup.com/idpl/article/7/2/76/3860948

671 The *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103INL) relating to robotic weapon's debate suggests three kind of human engagement: *human-in-the-loop,* in which robotics could act only under human commands; *human-on-the-loop* explained above and *human-out-of-the-loop,* in which robots could act autonomously without any human controls. This Resolution is available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN.

672 Recently, Italian Administrative Courts have promoted the idea that artificial intelligence should be used as tools, see *Tar Lazio*, *sez*. III *bis*, 4 April 2017, n. 4195; *Tar Puglia*, *Bari*, *sez*. I, 27 June 2016, nn. 806 and 807.

673 See E. CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica,* in *Giornale di Diritto Amministrativo*, 2, 2015, p. 4.

674 K. E. MARTIN, *Ethical implications and accountability of algorithms,* in *Journal of business ethics,* May 2018, p. 2. The author conceptualize that «algorithms create moral consequences, reinforce or undercut ethical principles, and enable or diminish stakeholder rights and dignity».

675 About this concern and its consequence, see R. BINNS, *Algorithmic accountability and public reason,* in *Philos. Technol.,* 2017, available at https://link.springer.com/article/10.1007/s13347-017-0263-5.

676 In the same sense, see G. PESCE, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, 2018, p. 235.

Building technical legal standards could be a first step to allow public bodies or judiciary courts to optimize external oversight. Therefore, it is valuable that the internal and external oversight can be developed together, in order to guarantee, «the former provides all the relevant information to the latter to evaluate the adopted decision».[678] Therefore, this proposal might empower rights of article 22nd GDPR, whose efficacy could be at risk without added technical legal standards.

The extension of good administration principle to the preliminary phase of artificial intelligence programming responds to the necessity to «balance the loss in comprehension and participation against the potential gains in outcomes and procedural fairness»[679]. At the same time, also impartiality could be respected: algorithmic construction is a «translation process»[680] so automated systems could replicate discrimination biases of humans.

Consequently, public bodies should prepare an impact assessment[681] to verify whether artificial intelligence works legally, as well as fairly. It could be a useful way to verify *ex post* the reasonableness and proportionality of administrative act. In addition to this proposal, public bodies could promote the use of distributed ledger technology (blockchain) in order to track every stage of algorithmic functioning.[682]

On the one hand, public bodies must control the programming of artificial intelligence[683], in order to preserve the good administration and impartiality principle. On the other hand, public bodies have to guarantee rights to participation and opposition, according to article 22nd GDPR. In this way, artificial intelligence could be used without concerns and they could be integrated in the existing constitutional and administrative system.

4. Public power and the content of some principles are changing. The use of ICT in public sector transforms the public power because of new tools, which allow public bodies to do something more. For example, the use of ICT throughout the city permits local government to reallocate financial resources in an efficiently way, more respectful of people's needs: as mentioned above, evidence-based government leads the planning of public services, indeed of traditional and authoritative way.

677 GOVERNMENT OFFICE FOR SCIENCE, *Artificial intelligence: opportunities and implications for the future of decision making*, 2016, p. 14 is really clear about the necessity of defining *ex ante* public benefit.

678 A. ROIG, *Safeguards for the right not to be subject to a decision based solely on automated processing (article 22 GDPR),* in *European Journal of Law and Technology,* 8, III, 2017, p. 9.

679 J. DANAHER, *The threat of algocracy: reality, resistance and accommodation*, cit., p. 13

680 R. KITCHIN, *Thinking critically about researching algorithms*, in *Information, Communication & Society*, 20, 2017, p. 22.

681 See some guidelines *Algorithmic impact assessments: a practical framework for public agency accountability*, by D. REISMAN, J. SCHULTZ, K. CRAWFORD, M. WHITTAKER, April 2018, available at https://ainowinstitute.org/aiareport2018.pdf. In which authors give rules for public bodies in order to use artificial intelligence legally as possible.

682 GOVERNMENT OFFICE FOR SCIENCE, *Artificial intelligence: opportunities and implications for the future of decision making*, 2016, p.16.

683 F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale,* in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 124 ss. Author argues that many rights are involved, such as right not to be discriminated, right to self-determination, consequently public bodies control that programmers respect ethic principles.

At the same time, the use of ICT in the administrative proceedings, such as the adjudicatory one, could rise some concerns about the safeguards of due process principle. In fact, the article 22nd GDPR provides some rights to recipients affected by automated decision-making, but they could be ineffective alone. For these reasons, in the ICT era, principles that lead public administration activity could be re-thought.

In particular, I suggest that public bodies could anticipate good administration and impartiality principle at the preliminary stage of artificial intelligence programming. Therefore, they could preserve legality in the functioning because of their own technical standardization. Thanks to this effort, not only recipients could understand how artificial intelligence works, but also judicial review could judge consciously.

At the same time, public bodies could prepare an impact assessment about the functioning of artificial intelligence, in order to verify *ex post* whether these tools could be used legally. It should be important that scholars identify some guarantees in order to correctly introduce artificial intelligences' outcome in the proceedings and to rethink categories of public purposes, suitability and proportionality of decisions.

Scholars have to lead the transformation of public administration in a deep and wide perspective, in accord to suggestion of legislators and Italian Digital Agency. In fact, at national level, Code of Digital Administration is the main source of law, which allow public bodies to make transition toward data revolution. For example, datasets are considered of national interest[684], some crucial national registers[685] are unified at national level and Italian Digital Agency conducts many efforts[686], in order to standardize[687] and rationalise informational public heritage.

These legislative tools could support public bodies to correctly deal with challenges and opportunities provided with information and communication technologies and give opportunities to scholars to comprehend the evolution of administrative law in the digital era.

ISABELLA ALBERTI

684 *D.lgs* december 30th 2010, n. 235 modified article 60th of Code of Digital Administration in order to make datasets of national interest wider.

685 National Registry of the Resident Population (*Anagrafe Nazionale della Popolazione Residente – ANPR*), National Registry of territorial data (*Repertorio Nazionale dei dati territoriali*), National Database of Public Procurement (*Banca Dati Nazionale dei Contratti Pubblici - BDNCP*)

686 For example it tries to make standardize and interoperable public datacenter; it gives some guidelines such as *Libro Bianco sull'Intelligenza Artificiale al servizio del Cittadino*. France makes a similar attempt with Report *Donner un sens à l'intelligence artificielle. Pour unestratégienationale et européenne*, 2018.

687 Nowadays, informatics coordination principle from article 117, 2nd paragraph, letter r) seems to prevail on the public administration autonomy principle, see F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità,* in *Diritto dell'Informazione e dell'Informatica,* 2, 2015, paragraph 4 in which he describes the legal and case law framework about this principle. See also, A. G. OROFINO, *L'esternazione informatica degli atti amministrativi*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione dell'amministrazione*, in D. SORACE, L. FERRARA, S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *A 150 anni dall'unificazione amministrativa italiana. La tecnificazione*, IV, Firenze, 2017, p. 195.

III.4

Government discretion in digitizing public administration – the Brazilian perspective*

SUMMARY: 1. Introduction. – 2. Time to change – public administration reform in Brazil. 2.1. Transparency. – 3. E-Government in Brazil. 3.1. E-Fiscal. 3.2. E-Banking. 3.3. E-Voting. – 4. Brazilian health system. 4.1. E-SUS. 4.2. Deficiencies of the Brazilian Healthcare System. 4.3. E-health card. 4.4. Medical E-files. 4.5. Civil engagement. 4.6. The protection of privacy. – 5. Chaos in the public healthcare system means increased litigation. – 6. Conclusion.

1. Since 2009, when the United States issued its Open Government Directive, improving public access to federal administration information, the world has seen a wave of transformation towards an open government philosophy, favoring transparency, efficiency, accountability, and public participation. In the sequence, the US issued the 'Digital Accountability and Transparency Act of 201'[688], and, more recently, the 'Providing Accountability Through Transparency Act of 2017'[689] prompting a worldwide proliferation of regulations that characterize a global trend towards Electronic Government.

These new winds quickly reached the Southern Hemisphere, bringing hope for improvement through an administration system less susceptible to fraud and corruption. Along with other American countries, Brazil has produced an incredible amount of legislation providing for the digitization of public proceedings and administrative procedures, enabling its entrance into the new digital era. However, some problems still have to be addressed.

First, one ought to consider whether this transition to a digitalized public administration is occurring horizontally or resulting in some sector being more favoredthan others, showing a government priority for strategic areas – such as the economic area –, causing the social area to lag way back. In fact, both the Brazilian Internal Revenue Service and the Brazilian Central Bank have long implemented the digitized process and completely integrated it within the realm of the 'Smart Government'.

Nonetheless, in the public healthcare sector – which is vital to materialize fundamental rights – the information is either not digitized, or when it is, it is done so poorly that it fails to help improve transparency. It is almost impossible for an ordinary citizen to obtain information on his or her own treatment, or else to understand why disclosure takes so long – or the reasons for it not to bedisclosed at all. Although countless data portals are available, there is no input of relevant data or else the available data outdated or inaccurate.

Secondly, the deficiency in digitizing data favors inefficiency and inequality. Considering that public healthcare in Brazil is subject to constitutional principles of equality, due process and universality – meaning that everyone is equally entitled to receive health assistance from the government through a regular administrative proceeding, with no preferences or privileges afforded to anyone – we wish to examine whether these constitutional mandates are actually being abided and whether the lack of transparency in the public healthcare system causes a high level of

688 Available from: <https://www.congress.gov/113/plaws/publ101/PLAW-113publ101.pdf>. Accessed on Aug 26 2018.

689 Available from: <https://www.congress.gov/bill/115th-congress/senate-bill/577>. Accessed on Aug 26 2018.

dissatisfaction among users, forcing them to go to court seeking clarification as to their standing in the waiting lists for surgery, hospital entry, and provision of medicine by means of injunctions demanding expedited treatment.

In fact, within the enormous number of new lawsuits filed every year in Brazil, a major part concerns the deficiencies of public health services and the disrespect of fundamental rights. To deal with this phenomenon of judicialization, the new Code of Civil Procedure[690] mandates that all legal case records are to be digitized. Since 2015, much computer software has been developed to allow faster case resolution, improving the administration of justice. Nonetheless, one ought to enquire whether all effortsdesigned for judiciary digitization will have a positive effect in the improvement of the health system itself.

The big challenge that the digitized era imposes is the protection of privacy. One ought to consider whether the Brazilian government is taking appropriate action to protect privacy in all digitized data – which includes personal data –, especially under the due process law clause, which requires proper notification of parties involved. In fact, this massive amount of digitized data produced by the public health system and the judiciary system is now open to the public at large and is available for research and reuse anywhere in the world. It is thus important to develop measures to secure this BIG DATA as it is not bound by border or jurisdiction constraints.

Lastly, considering that Brazil has had a broad and successful experience with electronic elections for the executive and legislative branches of power since 1996 and that this expertise could easily be used to engage the civil society in the decision-making process, one ought to examine whether the Brazilian government intends to enable democratic participation in social issues by giving due notice on forthcoming policies and the opportunity for comments.

In conclusion, we intend to demonstrate that Brazil has all the means necessary to be integrated as an e-Government through digitization and integration of all areas in public administration. Fundamental constitutional principles on the rule of law and public interest urge the implementation of the healthcare system along with equality, universality and due process, devoid of any discretionary policies aiming only at specific areas – such as taxation and financing –, as has been the case during past decades.

The real issue will be to create institutional constraints and to ensure that political decisionsupon implementing a high-quality e-healthcare system will apply efficiency, transparency and accountability principles to public action, thus meeting the expectations of Brazilian society.

2. It is common knowledge that Brazil is a huge country, it is the world's 5th largest country and has an estimated population of more than 206,1 million, an approved annual budget of R$ 3,5 trillion in 2018[691], and GDP [PPP] of $ 3,1 trillion reais. Considered the world's largest rain forest, Brazil is extremely rich in many different natural resources[692]. Although it occupies the 8th position

690*Paper prepared for presentation at the University of Milano Seminar"Big Data and Law: New challenges Beyond Protection", in October 2018.

Law 13,015 of July, 21, 2014. New Brazilian Code of Civil Procedure, Articles 193 through 199. Available from: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm>. Accessed on Aug 26, 2018.

691Available from: <http://agenciabrasil.ebc.com.br/politica/noticia/2017-12/orcamento-de-2018-e-aprovado-com-previsao-de-gastos-de-r-357-trilhoes>. Accessed on Aug 26, 2018.

692Available from: <https://www.heritage.org/index/country/brazil>. Accessed on Aug 26, 2018.

among the 10th largest economies in the world and a USD 1.8 economy[693], there is great social inequality and poverty among its population[694].

In addition, the Brazilian Constitution of 1988 expressly sets forth the Brazilian state's goals, namely: to build a free, just and equal society. This constitutes a major challenge as it requires that the government make social rights fully available for its population – which includes education, health, food, work, housing, leisure, security, social security, protection of motherhood and childhood, and assistance to the destitute[695], establishing the grounds for a welfare State, a social state, as defined by the Brazilian Supreme Court[696].

Such challenge and huge numbers called fora reform in the administrative branch. In 1996, the Brazilian government launched a Reform Plan[697], starting with the 19th amendment to the Constitution – which imbedded the principle of efficiency into the administration principles listed in article 37[698], all with a view to building astrong, social and democratic state. The Reform Plan was inspired by the New Public Management ideas, based on the principle that «governments could be managed like an enterprise"[699], so as to modernize and improve Brazilian public administration.

The global financial and economic crises of 2008, however, marked the end, or at least the reinvention of the NPM, with profound changes to «the establishment of a Smarter State that is fiscally sustainable»[700]with an emphasis on fostering efficiency, accountability, and transparency in government action, as well as the introduction of anticorruption practices, through investments in modern technological tools, such as Information Technology [IT].

693 Available from: <https://www.weforum.org/agenda/2017/03/worlds-biggest-economies-in-2017/>. Accessed on Aug 26, 2018.

694According to IBGE, 50 million Brazilian citizens live below the poverty line. Available from: <http://agenciabrasil.ebc.com.br/economia/noticia/2017-12/ibge-brasil-tem-14-de-sua-populacao-vivendo-na-linha-de-pobreza>. Accessed on Aug 26, 2018.

695 BRAZIL. Constitution of the Federative Republic of Brazil, 1988. Article 6. "Education, health, food, work, housing, leisure, security, social security, protection of motherhood and childhood, and assistance to the destitute are social rights, as set forth by this Constitution." Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf>. Accessed on Aug 26, 2018.

696 BRAZIL. Supreme Court (Ag. Reg. no RE) 1.101.106/DF. Reporter: Justice Celso de Mello. Brasília, August 9, 2018

697 Available from: <http://www.bresserpereira.org.br/rgp.asp>. Accessed on Aug 26, 2018.

698BRAZIL, Federal Constitution, 1988. Article 37. "The governmental entities and entities owned by the Government in any of the powers of the Union, the states, the Federal District and the Municipalities shall obey the principles of lawfulness, impersonality, morality, publicity, and efficiency." Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf>. Accessed on Aug 26, 2018.

699 G. Napolitano, *Looking for a smarter government (and administrative law) in the age of uncertaint,* in S. Rose-Ackerman, P. Lindseth, B. Emerson, *Comparative Administrative Law*, Cheltenham, 2017, II ed., p. 358.

700 Ibidem, 2017, p. 359.

III.4

Again, following the world openness trend inspired by the United States' Open Government Directive of 2009, Brazil launched the Transparency Act[701] – which provides on the access to public information and constitutes the framework for Brazilian E-government policies[702].

2.1. One of the first requirements for a modern 'Smart State' is to ensure transparency and openness in governmental activities. It is not easy to define *transparency*, however, as its concept is «expanding, becoming larger and more diffuse by incorporating more ideas into it»[703]. It is true that «Transparency limits corruption, protects against opportunistic behavior by officials and encourages public participation»[704].

Although many scholars define transparency simply as access to information, it surely encompasses much more than that.

«First, transparency is particularly about lowering the cost of physical access to information in real-time. «Transparency" or «access" does not really exist if obtaining and securing information is costly in either time or effort […]

Second, «transparency» has a computational or complexity dimension»[705]

In order to be transparent, a government has to make information available at a low cost and in real time, which means online, in the Internet. The burden is now on the government to open data, in order to make information ready for public access. Also, it is not only about the data, but the quality, the complexity of the data made available – that is, data which will enable people to find the right answers to the questions asked.

On the other hand, transparency encourages public participation with a view «to improving the democratic process and more informed agency deliberation"[706]. Although transparency provisions do not define the standards of said participation [but, of course, the more direct it is, the better], they include the participation of individuals and non-governmental groups - «the groups that will be affected by the administrative decisions»[707].

701 BRASIL. Law 12,527 of November 18, 2011. This law shall govern the access to information afforded by item XXXIII of Art. 5, item II of Paragraph Three of Art. 37, and Paragraph 2 of Art. 216 of the Federal Constitution; amends Law No. 8,112 of December 11, 1990; revokes Law No. 11,111 of May 5, 2005, as well as the provisions on Law No. 8,159 of January 8, 1991; and sets forth other actions that ought to be taken.Available from: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/l12527.htm>. Accessed on Aug 26, 2018.

702 F. S. O. S. Bonelli, *Administração pública contemporânea e Informática: o surgimento, os princípios administrativos envolvidos e os limites ao avanço do Governo Eletrônico no Brasil (e-Gov),* in Revista de Direito Administrativo contemporâneo: ReDAC, 2014, II 2, 9, jun. 2014, p. 13.

703 R. G. Vaughn, *Transparency in the Administration of Laws: The Relationship between Differing Justification for Transparency and Differing Views of Administrative Law*. American University International law review, v. 26, Issue 4, Article 3. p. 969, 2011 - Provided by Harvard Law School Library. Available from: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1719&context=auilr>. Accessed on Aug 26, 2018.

704 A. Candeub, *Transparency in the Administrative State*. 51 Houston Law Review, 2013, p. 386. Provided by Harvard Law School Library. Available from: <http://www.houstonlawreview.org/2013/12/06/512-transparency-in-the-administrative-state/>. Accessed on Aug 26, 2018.

705 Ibidem, 2013, p. 387.

706 Ibidem, 2013, p. 389.

707 R. G. Vaughn, op. cit., 2011, p.981.

III.4

Despite different doctrinal opinions, Bonelli argues that transparency has been incorporated into the Brazilian Constitution as a principle – when it refers to publicity and access to information – in article 5, XXXIII[708], as well as in article 37 and II, and paragraphs 2 and 3 of art. 216[709], which provides on the access to information concerning government actions[710]. The Brazilian Supreme Court has pointed in the same direction, stating that publicity is a «precept that recommends governmental transparent action»[711]; and transparency is a more specific aspect of the publicity principle[712], which renders it more concrete and gives the citizen the possibility to be aware of governmental action.

Transparency demanded openness of governmental information. Starting with the federal statute that governs public management responsibility[713], the federal government decided to implement transparency by issuing several acts whichaddressedits duty to disclose information on public finances [see the Transparency Federal Act[714]]. The Supreme Court, however, ruled that

708 BRAZIL. Federal Constitution, 1988. Art. 5. XXXIII – All individuals are entitled to obtain from public authorities any information of private interest to said individuals, or else of collective or general interest, and such information shall be disclosed within the timeframe provided by law, subject to liability penalties applicable to authorities addressed, except where such information is classified, as required by security concerns applying to society or the State. Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf>. Accessed on Aug 26, 2018.

709 BRAZIL. Federal Constitution, 1988. Art. 216. […] Paragraph Two. Public administration authorities shall manage government documents and afford consultation thereof to all who need it in the manner provided by law. Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf>. Accessed on Aug 26, 2018.

710 BRAZIL. Federal Constitution 1988. Art. 37. All direct or indirect public administration authorities of any of the branches of power of the Union, the states, the Federal District and municipalities shall abide by the principles of legality, impersonality, morality, publicity and efficiency and, further, by the following: […] Paragraph Three. The law shall provide as to the manner of user participation in direct or indirect public administration and shall specifically regulate: […] II – User access to administrative records and information on government action, due observance to be given to the provisions of art. 5, X and XXXIII. (our emphasis) Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf>. Accessed on Aug 26, 2018.

711 BRAZIL. Supreme Court. Writ of Mandamus (MS) No. 33,340/FD. Brasilia, May 26, 2015.

712 BRAZIL. Supreme Court. Direct Unconstitutionality Action (ADI) No. 2,444/RS. Brasilia, November 6, 2014.

713 BRASIL. Complementary Law No. 131 of May 27, 2009. Available from: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp131.htm>. Accessed on Aug 26, 2018.

714 BRASIL. Law 12,527 of November 18, 2011. Available from: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Accessed on Aug 26, 2018.

ensuing regulation proved to be «insufficient to deal with the problem»[715]. Concrete action and a change of mentality were needed.

Transparency is crucial in contemporary administrative governmentin a democratic society, especially when most of the population have access to Internet[716] and this calls for more interaction with government action[717].

It is important to mention that since 2004 the Federal Government has created a *Portal da Transparência*[718] that was totally renovated in 2018 – a cyberspace that should be able to «explain governmental action»[719], aiming the provide tools for the citizen to know and to question government activities, acting as a state controller, enabling social control of public expenditure and public management [which should be guided by legality and ethics, mindful of public interest][720].

The *Portal da Transparência* is just the beginning. Nonetheless, recent studies show that the portal is deficient because transparency is only more accurate when it relates to the «organizational structure» and the «programs and actions» of public institutions [and this includes the easiest information to deliver]; nonetheless, when it gets to financial information, such as «public expenses» and «contracts», disclosures are neither accurate nor clear. The conclusion is that «it is clear that transparency is not among the priorities for [Information] law implementation»[721]. Weknow well that, as Vaugahn warned, «all governments an most organizations exercise some discretion in determining what will be known and what will be kept in secret»[722].

3. As «[…] Governments around the world have realized the great potential of using Information and Communication Technologies [ICTs] to create so called «smart societies for social and economic development»[723], in 2012, Brazil gave the first steps towards the regulation of public

715BRAZIL. Supreme Court. Extraordinary Appeal (RE) No. 865,401/MG. Brasilia, August 14, 2015. SUMMARY: Constitutional Law. Fundamental right to access information of collective or general interest. Extraordinary appeal grounded on infringement of art. 5, item XXXIII of the Federal Constitution. Application filed by a city council member as city representative and as citizen, directly with the chief of the Executive Branch, with a view to securing information and documents concerning municipal management. Application denied. Invocation of the fundamental right to access information, calling for compliance with the duty to ensure transparency by public authorities, as well as principles governing the republic and publicity. Thesis of municipality grounded on undue interference, the separation of the branches of power and the difference between congressional prerogatives and congressmen prerogatives. General repercussion not acknowledged. Available from: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15338868743&ext=.pdf>. Accessed on Aug 26, 2018.

716 According to IBGE, a Brazilian statistical data institute, 48,1 million households have access to internet, a figure that represents 69.3% of all households in Brazil. Available from: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens.html>. Accessed on Aug 26, 2018.

717 F. S. O. S. Bonelli, op. cit., 2014, p. 24-25. Author´s translation

718 Available from: <http://www.portaltransparencia.gov.br>. Accessed on Aug 26, 2018.

719 R. G. Vaughn, op. cit., 2011, p. 971.

720 M. M. Ribeiro, C. O. de A. Freitas, *Análise crítica do e-government como instrumento de eficiência da arrecadação tributária, in* Revista de Direito Empresarial, 2012, p. 10.

721 T. C. Marinho, *Saúde Transparente: uma análise do cumprimento da Lei de Acesso à Informação nas instituições públicas federais de saúde*, 2017, p. 85. Available from: <http://bibliotecadigital.fgv.br/dspace/handle/10438/19480>. Accessed on Aug 26, 2018.)

722 Ibidem, 2017, p. 971.

record digitalization[724]. In 2000[725], the Brazilian government created a special group to develop electronic policies of interaction in all branches and levels of government administration, aiming at providing the universalization of services, accessible government, and advanced infrastructure.

After the world crises of 2008, the Brazilian federal government finally launched a digital government policy, aiming to provide for more administrative efficiency, access, and transparency, enabling the proximity of the society with the public services that are available[726].

The benefits of e-government by use of IT and technology are enormous as the latterincreasespopular participation, universalizes public services, and cuts costs[727] by focusing on basic principles such as equal access to social rights, openness and transparency, by favoring co-working, and by prioritizing digital services, security and privacy, social participation and control [as well as the government as a platform for innovation].

The power to define strategic goals for E-government [*Estratégia de Governança Digital – EGD*] was delegated to regulatory bodies of the Executive branch through the creation of the Governmental Digital Portal[728], which aims at improving government action towards citizens and gathering information on federal public policy in such a way as to facilitate public participation devoid of barriers.

As we will demonstrate below, digitalization policies have not been uniform for all areas. Some areas that are considered more strategic and vital - such as taxation and fiscal – have been totally integrated into the digital era. Nonetheless, social areas are lagging far behind and remain on their implementation stage.

3.1. In 1964, the Fiscal Federal Department created the first Federal Tax Database[729] with a view to regulating and implementing fiscal policies and rendering all tax information in Brazil uniform. In 1968, the first electronic tax returns were filled and all Brazilian citizens, whether taxpayers or not were assigned both a taxpayer number [*CPF – Cadastro Pessoa Física*] and a taxpayer identification card [*CIC*]. Since then, the system has seen much improvement[730].

723 M. I. Manda, J. Backhouse*, Towards a "Smart Society" Through a Connected and Smart Citizenry in South Africa: A Review of the National Broadband Strategic and Policy, in* H. J. Scholl, O. G. M. Janssen, B. K. Lindgren, I. Lindgren, P. P. E. Tambouris, M. A. W. T. Janowski, D. S. Soares. LENCC – Lecture Notes in Computer Science 9820 - Eletronic Government – *15th IFIP-WG 8.5 International Conference, EGOV 2016,* p.228, *Guimaraes, Portugal, September 5-8, 2016 Proceedings.* Switzerland, 2016- Provided by Harvard Law School Library.

724Available from: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm>.Accessed on Aug 26, 2018.

725Available from: <https://www.governodigital.gov.br/EGD/historico-1/historico>. Accessed on Aug 26, 2018.

726Available form: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8638.htm>. Accessed on Aug 26, 2018.

727 M. M. Ribeiro, C. O. de A. Freitas, op. cit., 2012, p. 3.

728Available from: <https://www.governodigital.gov.br/EGD>. Accessed on Aug 26, 2018.

729 BRAZIL. Federal Law nº. 4,516 of December 1st, 1964. This law establishes the Federal Data Processing Service, an entity linked to the Brazilian Finance Ministry. Available from: <http://www.planalto.gov.br/ccivil_03/LEIS/L4516.htm>. Accessed on Aug 26, 2018.

730Available from: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del0401.htm> <http://idg.receita.fazenda.gov.br/sobre/institucional/memoria/imposto-de-renda/historia/1968-a-1981-comeca-a-era-da-secretaria-da-receita-federal>. Accessed on Aug 26, 2018.

In 1997, the government created and implemented *Receitanet,* a web portal for individual taxpayers that afforded the electronic tax return filing option [no hard copy needed] to all. In 2013, the Brazilian Revenue Serviceprocessedmore than 25,571,747 e-tax returns, and in 2017, the number of taxpayers rose to 29,269,987[731] and in less than three months 10% of all tax returns had already been processed, and taxpayers started to receive whatever tax refunds they were entitled to.

All this efficiency is also seen in all levels of government where e-filingis afforded to all other kinds of taxes - including state and local taxes, all of them completely integrated into sophisticated software. As Ribeiro recalls, «if there is an area where e-government is really advanced, that area is tax administration» because it is «vital for the State»[732]. Information cross-examination is swifter and more accurate, and control is made easier through the use of electronic book-keeping. The entire fiscal obligation can be fulfilled and controlled through the Internet, and this boots tax revenue[733].

3.2. Due to the inflation that plagued Brazil in the 80's – causing interest rates to rise to as high as 84% a month –, all efforts were focused on controlling the inflation rate [which reached more than a whopping 707.4 per cent in 1985-9 period][734]. To face the challenges of its production and cope with financial market demands, the Brazilian banking and financial system entered the digital era in the mid 90', offering new digital services that conformed to federal regulations.

The Brazilian Central Bank developed a spectacular national payment system, which became one of the quickest fund-transfer, clearance and settlementsystems in the world. «[...] Internet banking became widely used: by the end of 2009, some 35 million cashing accounts could be accessed remotely via Internet – a figure that accounted for some 48% of all banking transactions in terms of volume that year»[735].

In 2016, Brazilian Central bank issued new regulations requiring digitalization of all banking transactions, even public banking institutions – such as Banco do Brasil, Caixa Econômica Federal, and BNDES, who are responsible for fostering public policies - are extremely efficient, offering the most sophisticated Internet sites, with total integration of products and services, with branches spread across almost every city in the country and overseas[736].

As a result, the Brazilian Banking system ranks 32nd in efficiency in the world financial system according to a World Economic Forum study[737], due to the fast digitalization of the financial system that started in the 80s.

In sum, a system that is totally integrated in the realm of the 'Smart Government' transition to a digitalized public administration.

731Available from: http://www.serpro.gov.br/menu/noticias/noticias-2018/mais-de-29-milhoes-de-declaracoes-do-irpf-2018-foram-entregues-no-prazo>. Accessed on Aug 26, 2018.

732 M. M. Ribeiro, C. O. de A. Freitas, op. cit., 2012, p. 10.

733 M. M. Ribeiro, C. O. de A. Freitas, op. cit., 2012, p. 11.

734 Available from: <https://www.jstor.org/stable/157697?seq=1#page_scan_tab_contents>. Accessed on Aug 26, 2018.

735 Payment, clearing and settlement systems in Brazil, CPSS – Red Book – 2011. Available from: <https://www.bis.org/cpmi/publ/d97_br.pdf>. Accessed on Aug 26, 2018.

736Available from: <https://www.export.gov/article?id=Brazil-Banking-Systems Accessed on 08.26.2018>. Accessed on Jun 23, 2018

737Available from: <https://exame.abril.com.br/economia/os-paises-onde-o-sistema-financeiro-funciona-melhor/>. Accessed on Jun 23, 2018.

3.3. Another area that deserves attention is the electoral area, as the Brazilian Constitution mandates a direct voting is to be in place as of 1988[738]. Brazil has developed incredible know-how in direct electronic elections – with modern software – «to ensure more transparency in the electoral process […] a symbol of credibility and democracy» [e-voting [739]], thus guaranteeing direct political participation for the citizen.

In 2014, more than 140 million citizens were able to use e-voting for presidential elections, and the resultswere disclosed in a matter of hours the very same day. The same happened throughout the country for governor and mayor election, alongwith all the legislative representatives.

This successful experience in electronic elections, with e-voting machines, for the executive and legislative branches could easily be used to obtain civil society participation in the decision-making process in the social areas as well.

4. The Brazilian Constitution promulgated in 1988 establishes that healthcare is a social right[740], as well as «a right for all, and a duty for the State, and shall be guaranteed by means of social and economic policies», which means that all 200 million Brazilians should have equal access to the public healthcare system [ranking as the largest public health system in the world[741]].

The approved federal healthcare system budget for 2018 was R$ 130 billion and is expected to service more than 60% of poor – which depends solely on the public system *[SUS]* for primary care, and 90% for secondary and tertiary care.

In order to cope with this enormous duty, constitutionalistsconceived a unified healthcare system" [*Sistema Único de Saúde – SUS*] with a view to supervising and controlling medical procedures, products and substances of interest to healthcare and to participate in the production of drugs, equipment, personal and sanitation actions, among other things[742]. To achieve its objectives, several statutes were promulgated to regulate said unified healthcare system - *SUS*[743].

738 BRAZIL. Federal Constitution, 1988. Article 14. The sovereignty of the people shall be exercised by universal suffrage and by the direct and secret voting, with equal value for all, and, according to the law. Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf> . Accessed on Aug 26, 2018.

739Available from: <http://www.tse.jus.br/imprensa/noticias-tse/2014/Junho/conheca-a-historia-da-urna-eletronica-brasileira-que-completa-18-anos>. Accessed on Aug 26, 2018.

740Article 6. "Education, health, food, work, housing, leisure, security, social security, protection of motherhood and childhood, and assistance to the destitute are social rights, as set forth by this Constitution." Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf> . Accessed on Aug 20, 2018.

741 See: National Health Covenant. Available from: <http://bvsms.saude.gov.br/bvs/publicacoes/pacto_nacional_saude_mais_medicos.pdf>. Accessed on Aug 26, 2018.

742 BRAZIL. Federal Constitution, 1988. Art. 200. […] It shall be incumbent upon the Unified Healthcare System, among other duties and as provided by law, to: […]. Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf> . Accessed on Aug 26, 2018.

743 BRAZIL. Law No. 8,080 of September 19, 1990. This law provides on conditions necessary to promote, protect and recover health, as well as on the organization and the functioning of services applying thereto, and sets forth other actions that ought to be taken. Available from: <http://www.planalto.gov.br/ccivil_03/leis/L8080.htm>. Accessed on

Although Brazil spends 9% of its GDP in public healthcare[744], these funds made available seem to never be enough. The major obstacles for better healthcare – an area in which it can mean the difference between life or death – are the lack of information and corruption.[745]. Currently, there are 5,530 public hospitals in Brazil, with 336,941 hospital beds, including intensive care, for hospital entry – a figure that includes all federal, state and municipal hospitals, as well as emergency care units[746].

4.1. The Unified Healthcare System government portal enables access to e-*SUS*[747], a kind of software that was developed to collect, simplify, manage and use healthcare information, aiming at the integration of healthcare professionals and the population. e-*SUS* includes e-*SUS-AB*[748], which is an integrated system of primary healthcare for all the municipalities in Brazil that was developed to modernize and restructure all the information system, aiming at the improvement of healthcare provided to the population[749].

The healthcare system includes a branch for the primary healthcare, family doctors, specialists, pharmacy, laboratories, home care, daycare, and Hospital Care with a Hospital Database – HIS – [Hospital Information System]. All units should be computerized to enable access to electronic medical records [*PEP – Prontuário Eletrônico do Paciente*].

Although e-SUS represents great improvement in the healthcare system, government investments in IT, equipment and training personnel have been neither sufficient nor proportional to the needs of the population. Despite the efforts to implement e-SUS, in reality the conclusion is dramatic: «Brazil is far from a true e-healthcare system, hence the importance of developing a clear and complete strategy for the sector»[750].

Aug 26, 2018.

BRAZIL. Law No. 8,142 of December 28, 1990. This law provides on community participation in management of the Unified Healthcare System (SUS) and on intergovernmental transfer of funds intended for healthcare, and sets forth other actions that ought to be taken. Available from: <http://www.planalto.gov.br/ccivil_03/LEIS/L8142.htm>. Accessed on Aug 26, 2018.

BRAZIL. Decree No. 7,508 of June 28, 2011. This decree regulates Law No. 8,080 of September 19, 1990, so as to provide on the organization of the Unified Healthcare System (SUS), the planning of healthcare, the assistance to health and the inter-federal coordination, and sets forth other actions that ought to be taken. Available from: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7508.htm>. Accessed on Aug 26, 2018.

744Available from: <https://www.theatlantic.com/health/archive/2014/05/the-struggle-for-universal-healthcare/361854/>. Accessed on Aug 26, 2018.

745 T. C. Marinho, op. cit., 2017, p. 14. Author´s translation

746 Available from: <http://www.conass.org.br/consensus/numero-de-hospitais-brasil-sus/>. Accessed on Aug 26, 2018.

747 Available from: <http://www2.datasus.gov.br/ESUSHOSP/>. Accessed on Aug 26, 2018.

748Available from: <http://bvsms.saude.gov.br/bvs/saudelegis/gm/2013/prt1412_10_07_2013.html>.AccessedonAug 26, 2018.

749 J. P. Alves, Í. V. A. Diniz, K. T. G. França, L. M. da Silva, C. S. Martiniano, *Avanços e Desafios na Implantação do e-SUS-Atenção básica*, 2018, p. 3. Available from: <http://www.editorarealize.com.br/revistas/conbracis/trabalhos/TRABALHO_EV071_MD4_SA7_ID788_15052017202831.pdf>. Accessed on Aug 26, 2018. Author´s translation

750 R. M. E Sabbatini, *e-Saúde,* in P. T. Knight, C. C. C. Fernandes, M. A. Cunha, *E-Desenvolvimento no Brasil e no mundo* – subsídios e programa e-Brasil. Camara-e.net - Câmara Brasileira de Comércio Eletrônico - YENDIS, 2007, p. 751. Available from: <http://www.sabbatini.com/renato/papers/e-saude.pdf>. Accessed on Aug 26, 2018. Author´s translation.

4.2. Although Brazil spends more than 9% of its PPP in healthcare[751], the level of dissatisfaction in its population is very high, and we can point out many reasons, starting with the size of the Brazilian territory and infrastructure deficiency, as well as a lack of trained healthcare professionals, «corruption and inefficiency»[752], all of which could certainly be minimized through the effective implementation of e-health in the public sector [753].

Implementation of e-healthcare through e-SUS would certainly help to improve the healthcare system, but «medical care has been one of the last areas to have adopted the modern ITC in its routines and proceedings. One of the main causes for this delay is the cultural obstacle represented by healthcare professionals, who until just recently still ignored or were refractory to such progress»[754].

Another major problem for implementing e-health is the lack of a computerized structure in the healthcare system – only 52% of SUS units have computers and only 36,7% have access to the Internet[755]–, as well as hardware and software incompatibility. More investment in SUS unit computerization and proper personnel training [to ensure proper use of the new technology made available] is needed to overcome the first implementation stage of the process [756].

Another challenge is to provide clear and accountable information, allowing its integration and sharing, which is the foundation for an efficient e-health system. Healthcare webportals do not provide objective data, and the information provided is not sufficient to make the population aware of its rights[757].

One of the most common complaints of the population is the lack of primary assistance in public hospitals. Users of the healthcare system never know if or when the doctor will be there for assistance or surgery, and if or when they will receive treatment or prescribed medicine. There are never enough hospital beds for patients, and it is not uncommon to see people receivingmedical treatment in chairs, at the hall entrance or corridors of the public hospitals. There is no therapy offered for terminal patients, who are invariably sent back hometo die with their family, devoid of either assistance or dignity.

Moreover, the amount of waiting time prior to surgery is a serious complaint.According to the Federal Medical Counsel, in 2017, there were more than 900,000 Brazilians in the waiting list for

751 Available from: <http://agenciabrasil.ebc.com.br/economia/noticia/2017-12/gastos-com-saude-crescem-mesmo-em-meio-crise-e-atingem-91-do-pib>. Accessed on Aug 26, 2018.

752 T. C. Marinho, op. cit., 2017, p. 9. Author´s translation

753 J. P. Alves, Í. V. A. Diniz, K. T. G. França, L. M. da Silva, C. S. Martiniano, op. cit., 2018, p. 5.

754 R. M. E Sabbatini, op. cit., 2007, p. 741. Author´s translation

755 J. P. Alves, Í. V. A. Diniz, K. T. G. França, L. M. da Silva, C. S. Martiniano, op. cit., 2018, p. 3.

756 E.H. DINIZ, *O governo eletrônico no Brasil,* Revista de Administração Pública. Rio de Janeiro, 2009. Available from: <http://www.scielo.br/scielo.php?pid=S0034-76122009000100003&script=sci_abstract&tlng=pt>. Accessed on Aug 26, 2018.

757There are many proposal under discussion to alter the law that regulates health system, to open information concerning the lines for treatment. See: Projeto de Lei do Senado (PLS) nº 192, de 2018. Available from: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133007>. Accessed on Aug26, 2018.

See also Senate Bill (PLS) nº 393 of 2015. Available from: <https://www12.senado.leg.br/noticias/audios/2017/08/transparencia-em-fila-de-cirurgia-vai-acabar-com-privilegios-no-sus-diz-otto-alencar>. Accessed on Aug 26, 2018.

different types of surgery with no expected date in sight. Although patient position in line can be known, the information provided by healthcare web portalsis totally insufficient for it does not provide either clear information on the expected waiting time or scheduled medical procedures. People end up passing while still in the waiting list before getting to undergo the procedure needed[758].

The Federal Government implemented a healthcareregulation systemcalled *SISREG*[759] aiming to integrate, organize and discipline the waiting lines for primary assistance, hospital admission and surgeries [available in all three levels of health units]. The idea was that a patient would be able tokeep track of their position in the line through an app *[Meu Digi SUS]*. However, in reality the system is not available for all units, as it covers less than 1/3 of all municipalities, with only 204 ambulatorial regulation centers and 19 hospital regulationcenters – which is not enough to meet demand[760]. Furthermore, as there is no control or supervision, healthcare units do not respect the lines. The system ends being unreliable, as the number of lawsuits filed has shown.

Regulation should be more stringent specifically for cancer treatment, as federal Law 12,732/12 stipulates a 60-day deadline to start treatment[761]. However, in 2014, only in the state of Rio de Janeiro over 500 individuals had been waiting for more than a year for treatment. The Brazilian Department of Justice *[Ministério Público]* sued the federal, state and local governments seeking proper enforcement of the law and calling for organized waiting lines and proper treatment[762].

It is also not clear why some surgery lines run faster than others. Sometimes patients in need of a knee surgery may wait longer than those who need backbone surgery, with neither explanation nor accurate information being given. This single example shows that the lines are not managed in a clear or transparent way, favoring corruption and fraud. Frequent scandals involving surgery lines, even in transplant lines, exposes the scenario[763].

Another huge problem involves medicine procurement in public hospitals[764], which involves a lack of transparency in the system. The Federal Government issues a list of medicines that are to be dispensed in public hospitals and public pharmacies.Until 2010, there were only 500 basic drugs in the list. In 2017, this number rose to 869 different drugs as included in the list[765]. It is not unusual to seelawsuits being filed in order to receive the medication prescribed by public hospital doctors

758 Available from: <https://portal.cfm.org.br/index.php?option=com_content&view=article&id=27314:crise-no-sus-brasil-tem-mais-de-900-mil-cirurgias-eletivas-represadas&catid=3>. Accessed on Aug 26, 2018.

759Available from: <https://www.servicos.gov.br/servico/cadastrar-se-no-sistema-de-regulacao>. Accessed on Aug 26, 2018.

760Available from: <http://www2.datasus.gov.br/DATASUS/index.php?acao=11&id=30430>. Accessed on Aug 26, 2018.

761 Available from: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12732.htm>.Accessed on Aug 26, 2018.

762 See Public Civil Action. Case No. 00067445-1.2014.4.02.51.01. 15th Federal Court in Rio de Janeiro. Available from: <http://procweb.jfrj.jus.br/portal/consulta/resconsproc.asp>. Accessed on Aug 26, 2018.

763 Available from: <https://g1.globo.com/rj/rio-de-janeiro/noticia/desvio-de-dinheiro-do-into-prejudica-milhares-de-pacientes-que-esperam-por-uma-cirurgia-na-unidade-de-saude.ghtml>. Accessed on Aug 26, 2018.

764Available from: <http://portalarquivos2.saude.gov.br/images/pdf/2017/maio/26/1.a-Banco-Mundial-Eficiencia-do-Gasto-com-Saude-CIT.pdf>. Accessed on Aug 26, 2018.

765Available from: <http://portalfns.saude.gov.br/ultimas-noticias/1727-ministerio-da-saude-publica-nova-lista-de-medicamentos-essenciais-para-o-sus>. Accessed on Aug 26, 2018.

[medicine included in the list but not available to be delivered to patients, with no neither reasonable nor timely justification being given].

The implementation of e-health would help to improve the efficiency and transparency in the public healthcare system, but it would depend more than anything on political will to invest on IT and infrastructure[766], as has already been done in other areas of government.

4.3. Albeit created in 2011 as an «ambitious project» to give each citizen a National Healthcare Card, a personal digital identification health card allowing identification and use of the healthcare system[767], until today the population is not aware of the importance of the using the SUS-card.

The implementation of the e-health card would bring benefits in terms of management and planning to the whole healthcare system, allowing its reorganization, with more efficiency and accountability, permitting the interconnection of information on doctor appointments and surgery, as well as medication prescription and medical e-files.

Improvement of the healthcare system depends on total integration of the e-health card at all levels of healthcare: federal, state and municipal[768]. It is impossible to understand why a country that has had a taxpayer identification card [CPF] for each citizen since 1996 has so much difficultyin implementing a similar card in its healthcare system.

4.4. Medical e-files *[PEP – Prontuário Eletrônico do Paciente]* represent a major evolution in e-health as they can store all of a patient's medical data, laboratory tests, clinical assistance, diagnoses, and treatment; plus, they can be sharedby doctors and hospitals, regardless of distance or patient location. Another advantage is that they prevent medical procedure and test result duplicity and are thus an excellent, cost-saving tool.

Although federal law mandates the use of electronic healthcare records, said useis still a dream in Brazil. Studies show that medical e-files are effectively used in «less than 1% of Brazilian hospitals»[769].

Unbelievable as it may seem, in Brazil, in 2018, patient healthcare records are still hand written, unavailable, incomprehensible, and subject to fraudulent alterations. Just as is the case with hospital formsand medical prescriptions, both filled out on paper, by hand and subject to all sorts of damage and inaccuracy. Bills designed to improve the use of electronic files are still in Congress[770], pending approval, without urgency, despite the fact that they would bring substantial benefits, affordingquality, organization, safety, and efficiency to the whole system. Sabbatini believes that «In the future, we hope that the core for e-health development in Brazilwill come with web-based medical e-files»[771].

766 R. M. E. Sabbatini, op. cit., 2007, p. 752.
767 R. M. E. Sabbatini, op. cit., 2007, p. 747.
768 R. M. E. Sabbatini, op. cit., 2007, p. 757.
769 R. M. E. Sabbatini, op. cit., 2007, p. 743. Author´s translation.
770Available from: <https://www12.senado.leg.br/noticias/materias/2018/04/03/aprovada-digitalizacao-de-prontuarios-medicos-em-hospitais>. Accessed on Aug 26, 2018.
771 R. M. E Sabbatini, op. cit., 2007, p. 755.

4.5. As we mentioned above, most public healthcare users in Brazil are among the poor [invariably illiterate individuals, considering that more than 7% of the Brazilian population has no access elementary education, a percentage that rises to 13,8%[772] in the northeast region]. This factor contributes tremendously to the lack of civil engagement in the decision- making process. Poor people don't participate. They are either not heard or heard only when the consequences are serious and get the attention of big media – namely, when people die because of lack of assistance.

To make matters even worse, we now see the rise of a social phenomenon called «digital exclusion», which is the inability to access the Internet and digital technology due to the high cost of equipment[773]and to use sophisticated technology. As only 69,3% of households in Brazil have Internet access [roughly 48,1 million households], we can infer that the population has limited access to e-government web portals and will be even farther from any information at all, a fact that will cause even greater social exclusion.

This means that the e-Government project demands not only public investment in technology within the administrative branch but also the provision of public computers and Internet access to poor communities to make e-government accessible to the population[774].

Popular participation could easily be achieved at all levels of government through direct participation in public hearings, referenda and plebiscites – tools already afforded by the Brazilian constitution[775].

There is also a provision requiring popular participation in the *SUS* Management Board on federal Law 8,142/90[776], a provision that could enable public policy control and supervision. Cruz emphasizes that reinforcing social participation in public healthcare policy-making will be valued as a political decision, affording power to allow growth in the universalization and equal access to healthcare, thus constituting a great opportunity for the active and creative insertion of the population in the promotion of public healthcare[777].

The reality is that popular participation and control are not effective due to lack of information and multiple conflicting interests that subtract power from society.[778]

In short, we could conclude that it is urgent to find a way to give voice to the poorto improve citizen engagement, participation and community collaboration. The mechanisms for effective popular participation, whether legal or technological, already exists in Brazil, and it is now up to politicians to decide whether they want to enable democratic participation by disclosing forthcoming policies and giving the opportunity for comments.

772Available from: <http://agenciabrasil.ebc.com.br/educacao/noticia/2017-12/taxa-de-analfabetismo-no-pais-na-faixa-de-15-anos-ou-mais-foi-de-72-em-2016>. Accessed on Aug 26, 2018.

773 M. M. Ribeiro, C. O. de A. Freitas, op. cit., 2012, p.11.

774 F. S. O. S. Bonelli, op. cit., 2014, p. 33.

775 BRAZIL. Federal Constitution, 1988. Article 14. The sovereignty of the people shall be exercised by universal suffrage and by the direct and secret voting, with equal value for all, and, according to the law, by means of: I – plebiscite; II – referendum; III – people's initiative. Available from: <http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf>. Accessed on Aug 26, 2018.

776 Available from: <http://www.planalto.gov.br/ccivil_03/LEIS/L8142.htm>. Accessed on Aug 26, 2018.

777 Available from: <http://www.scielo.br/pdf/sausoc/v21n4/v21n4a25.pdf>. Accessed on Aug 26, 2018.

778 Available from: <http://www.scielo.br/pdf/sdeb/v37n96/16.pdf>.Accessed on Aug 26, 2018.

4.6. The big challenge imposed by digitization lies on the protection of privacy. It yet remains to see whether the Brazilian government is taking appropriate measures to protect the privacy of all digitized data [data that includes personal data, especially under the due process law clause, which requires that due notice to be given to parties involved].

In fact, there isa massive amount of digitized data – produced by the public health system and the judiciary system – that is currently available for public scrutiny, research and reuse all over the world. As BIG DATA is not subjected to either international border or jurisdiction limits, it is important to develop measures to ensure its confidentiality.

Medical e-files call for much attention, especially in terms of privacy, security and ethical issues involving the use of open data [just as is the case in any other field]. The basic precautions such as providing username and password to login into the system and have access to the health information ought to be taken.

5. Although the last decade has seen much improvement ine-government, the great deficit in the social area, especially in the healthcare system, where poor people have been suffering directly from the inefficiency and lack of transparency, has made it necessary for citizens to go to court to secure their rights through injunctions, orders and explanations for lack of treatment.

When the first cases reached the Supreme Court, the court held that fundamental rights had not been afforded to those entitled to them and that Government could refrain from meeting its obligation to provide healthcare to citizens, as mandated by article 196 of the Brazilian Constitution[779]. This reliance on courts and judicial means for addressing these matters became known as healthcare judicialization.

According to the National Board of Justice *[Conselho Nacional de Justiça]*, in 2016, there were more than 1,346,931 pending cases involving healthcare. In 7 years, there was a 1.300% increase in the number of lawsuits of the cases involvingdrug dispensing, a situation that made it necessary for the government to create the National Health Forum in the Justice system[780] to monitor these lawsuits and diagnose the deficiencies in SUS through studies geared toward the development of solutions designed for improving the healthcare system. Healthcare comities were created, and federal courts have become specialized in healthcare cases[781].

779 'This court has already ruled that, despite the merely programmatic nature of art. 196 of the Federal Constitution, the State cannot refrain from complying with its duty to make available the means necessary for full enjoyment of the right to healthcare by citizens. Accordingly, due attention ought to be given to the following summary of the individual ruling entered by Justice Celso de Mello in extraordinary appeal (RE) no. 271,286: 'The right to healthcare is not only a fundamental right afforded to all individuals but also a constitutional consequence inseparable from the right to life. Public authorities, regardless of their institutional rank within the organization of the Federal Republic of Brazil, cannot ignore problems affecting an individual's health without engaging – even through omission - in a shameful unconstitutional behavior.' Available from: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=335538>. Accessed on Aug 26, 2018.

780Available from: <http://www.cnj.jus.br/busca-atos-adm?documento=2831http://www.cnj.jus.br/programas-e-acoes/forum-da-saude>. Accessed on Aug 26, 2018.

781 National Council of Law (BR). Resolution No. 238 of September 6, 2016. This law provides on the creation and maintenance of State Healthcare Councils by Trial Courts and Federal Regional Courts, as well as on the creation of specialized trial courts in cities having more than one tax court. Available from: <http://www.cnj.jus.br/busca-atos-adm?documento=3191>. Accessed on Aug 26, 2018.

III.4

Statistics show that the judicial branch of power has become the actual manager of public healthcare policies through the issuance of preliminary injunctions. Again, the Supreme Court ruled in favor of the citizens, holding that the judicial branch can rule on the implementation of the healthcare system, and that by doing so no infringement of the system of checks and balances results [separation of the branches of power clause][782].

The vast majority of cases involve individual rights and seek the provision of medicine or treatmentby public hospitals. The endless lines for surgery and hospital admission are questioned. The scenario was so dramatic that the Supreme Court ruled that all the three levels of government, federal, state and municipal are jointly and severally liable for healthcare[783].

Considering the tremendous quantity of individual healthcare cases and the collective interest involved, the Supreme Court is now deciding whether the Brazilian department of Justice has the standing to file class actions involving healthcare[784]. Said court is also deciding whether the judicial branch of power can or not control government expenditure on healthcare when the Constitution requires that state and local authorities allocate a minimum percentage of public funds[785] for public healthcare actions and services.

To deal with the judicialization phenomenon, the judicial branch had to readapt its systems, as the new code of civil procedure mandates all the judicial files are to be digitized. Since 2015, computer programs have been developed to improve the administration of justice.

782 BRAZIL. Supreme Court. Bill of Review on Suspension of a Preliminary Injunction (SL-AgR) No. 47/PE. Reporter: Justice Gilmar Mendes. Plenary. Brasilia, April 30, 2010. SUMMARY: Suspension of a Preliminary Injunction. Bill of Review. Public health. Fundamental social right. Art. 196 of the Federal Constitution. Public hearing. Unified Healthcare System (SUS). Public policies. Judicialization of the right to healthcare. Separation of the branches of power. Parameters for judicial resolution of concrete cases involving the right to healthcare. Joint responsibility of entities of the Federation in matters concerning health. Mandate to regularize the services provided by a public hospital. No evidence of serious lesion to public order, to the economy, to health and public security. Possible reverse damage. Bill of Review denied. Available from: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=610254>. Accessed on Aug 26, 2018.

783See the *leading case* (Theme 793 of STF decisions): EXTRAORDINARY APPEAL. CONSTITUTIONAL AND ADMINISTRATIVE SUBJECT MATTER. THE RIGHT TO HEALTHCARE. MEDICAL TREATMENT. JOINT RESPONSIBILITY OF ENTITIES OF THE FEDERATION. GENERAL REPERCUSSION ACKNOWLEDGED. REAFFIRMATION OF CASE LAW. Proper medical treatment for those who need it is one of the duties of the State, as it constitutes a responsibility for entities of the Federation. Defendants may be any one of such entities either severally or jointly. Available from: <http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4678356&numeroProcesso=855178&classeProcesso=RE&numeroTema=793>. Accessed on Aug 26, 2018.

784 Available from: <http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verPronunciamento.asp?pronunciamento=3307461> Accessed on Aug 26, 2018.

785 BRAZIL. Supreme Court. Extraordinary Appeal (RE) No. 858,075/RJ. Reporter: Justice Marco Aurelio. Brasilia, June 16, 2015. SUMMARY: BUDGET – PROVISION OF MINIMUM FUNDS FOR HEALTHCARE – JUDICIAL CONTROL – SEPARATION OF THE BRANCHES OF POWER – SCOPE OF ART. 2, ART. 160, SOLE PARAGRAPH, ITEM II, AND ART. 198, PARAGRAPHS TWO AND THREE OF THE PERMANENT TEXT, AND ART. 77, ITEM III, PARAGRAPHS THREE AND FOUR OF THE FINAL AND TRANSITIONAL PROVISIONS OF THE FEDERAL CONSTITUTION OF 1988 – EXTRAORDINARY APPEAL – GENERAL REPERCUSSION ACKNOWLEDGED. Available from: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28RE%24%2ESCLA%2E+E+858075%2ENUME%2E%29+OU+%28RE%2EPRCR%2E+ADJ2+858075%2EPRCR%2E%29&base=baseRepercussao&url=http://tinyurl.com/q3nvgsn>. Accessed on Aug 26, 2018.

Nonetheless, whether judicial branch endeavors have a positive effect in improving the healthcare system itself issubject to debate. Perhaps, it would be simpler for administrative healthcare authorities to implemented public healthcare policies themselves.

6. We hope that this paper contributes to the debate in two ways; first, by demonstrating the improvement of Brazilian public policies geared towards 'Smart Government' and our government's entrance into the e-Government era; and, secondly, by demonstrating that legislative efforts are not enoughif not coupled with concrete actions designed for improvement, especially in the healthcare area.

Brazil has established a reform plan to modernize its administration and its entrance in the E-Government era. Nonetheless, digitization of public administration is far from being uniform and has been more favorable to financial areas – such as taxation and banking, which nowadays are totally integrated and digitalized – and caused social areas to lag far behind.

As we have demonstrated, Brazil – a country currently managing the biggest public healthcare system in the world – now faces a huge challenge; namely, to ensure that all of its citizens get to fully enjoy their social rights, including the right to healthcare, under the principles of universality and equality.

The constant dissatisfaction of the population with the Brazilian healthcare system is visible. Many structural problems - such as the lack of transparency – remain unsolved. Individuals have the right to know when treatment will begin and when they will receive medicine; yet, in practical terms, healthcare records are inconsistent, and information is insufficient. The implementation of a digitized healthcare system is still in its inception, with medical records still being made in hard copy with no integration among healthcare units and no dissemination of the healthcare national card.

Furthermore, fundamental constitutional principles of rule of law and public interest require transparency in a modern administration. All the legislative efforts for fostering transparency and e-government will be worthless if data input is not accurate.

No technological tools will be enough if there is not a change in mindset, that is, one that favors disclosure of data on public spending and allows real participation of the population in the decision-making process and its control of government action with a view to achieving efficiency and curtailing corruption.

In short, e-government in Brazil can be successfully achieved if the government has the political will to prioritize social areas by integrating the poor – so that they may benefit from the use of electronic systems –, providing equipment and trained personal to educate individuals, implementing the program and preventing further digital exclusion.

CARMEN SILVIA LIMA DE ARRUDA