ISSN 2384-9169
Fascicolo n. 1 - 2021
rivista.eurojus.it

To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within the EU

DI FRANCESCO ROSSI DAL POZZO* E LAURA ZOBOLI**

SUMMARY: 1. Introduction. – 2. The constitutionalization of the right to the protection of personal data. – 2.1. The balancing act between the protection of data and their use in the public interest. – 3. The definition of personal (and non-personal) data in the EU regulatory system. – 4. Conclusions.

1. Introduction

The European data economy represents a vibrant and dynamic scenario where regulators and judges cover a crucial role, constantly catching up with the intense rate of innovation brought about by the ongoing digital revolution.

In particular, the Court of Justice of the European Union (CJEU) often had to interpret existing rules in order to adapt them to the digital evolution and to the data economy – striking a balance between interests that the regulator had not addressed yet. To date, however, several *ad hoc* pieces of regulation have been adopted at the EU level. In particular, the legislator's approach relies on differentiating between the various types of data being dealt with: personal data, non-personal data, private data and public data. In addition, sectoral regulations – thus relating to specific market sectors – have been given space.

This contribution intends to focus on personal data, to discuss critically a definition of personal data and the conditions for personal data protection to apply.

* Full Professor of European Union Law, University of Milan.
** Assistant Professor of European Economic Law, University of Warsaw. Laura Zoboli acknowledges the support of the National Science Centre, Poland (decision UMO-2018/31/B/HS5/01192).
Albeit the unitary conception of the manuscript, Francesco Rossi dal Pozzo drafted paragraphs 1 and 2 and Laura Zoboli drafted paragraphs 2.1, 3 and 4.

This matter is of paramount importance also considering that, in recent years, there has been an exponential growth in terms of quantity, quality and diversity of personal data processing activities, with an increasing tension between the need to protect the individuals to whom the processed data refer and that of guaranteeing the circulation of information for social, economic and public security purposes.

Hence the difficulty in delimiting the discipline on a conceptual as well as applicative level, also due to the heterogeneity of the possible purposes for which personal data are lent.

Therefore, this article intends to elaborate on the still ongoing evolution of the definition of *personal data protection* within the European Union system, considering both the CJEU's rulings and the current regulatory framework.

To do so, first, one has to consider the constitutionalization of the personal data protection elaborated by the CJEU and the boundaries between the protection of personal data and further fundamental rights. (paragraph 2). In this context, in light of the current Covid-19 pandemic, it was also considered important to devote a brief sub-section of this article to the balance between public health concerns and the protection of personal data as a fundamental right (paragraph 2.1). Second, it is crucial to reconstruct the definition of personal data within the current regulatory system so to understand its scope of application (paragraph 3). In doing so, it is also important to take non-personal data into consideration, since they are defined *a contrario*, that is, with a formula based on the definition of personal data. As it will be discussed in the concluding section of this paper, the analysis of both the case law and of the regulatory framework allows to identify an enlargement of the scope of application of the personal data category and protection within the EU (paragraph 4).

2. The *constitutionalization* of the right to the protection of personal data

As of today, the right to the protection of personal data is a fundamental right in the EU[1] and plays an important role in the holistic development of individuals.[2]

In order to define the boundaries of the protection of personal data, it is essential to retrace the path followed by the CJEU toward the *constitutionalization* of the right to the protection of personal data. Indeed, the activity of the CJEU has been (and still is) crucial for the evolution of the personal data protection. In the field, the Court acted – and acts – not only as a judge watching over EU integration, but also as a "constitutional guardian" of the European Union system, against threats both within and beyond its borders.[3] In certain circumstances, this pushed the Court to affirm the centrality of the protection of personal data, even in the presence of security instances.[4] Today, in light of the adoption of the General Data Protection Regulation

[1] Article 8 of the Charter of Fundamental Rights and Convention 108 of the European Convention on Human Rights. While in other States it is not; see P. M. SCHWARTZ and D. J. SOLOVE, *Reconciling Personal Information in the United States and European Union*, 102 *California Law Review*, 2014, 877.

[2] See J. RAUHOFER and C. BOWDEN, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, University of Edinburgh School of Law Research Paper Series No 2013/28, 17.

[3] See M. CARTABIA, *Convergenze e divergenze nell'interpretazione delle clausole finali della carta dei diritti fondamentali dell'Unione europea*, *Rivista Associazione Italiana Costituzionalisti*, 2, https://www.rivistaaic.it/images/rivista/pdf/3_2017_Cartabia (last access 31 January 2021).

[4] See F. FABBRINI, *Privacy and National Security in the Digital Age*, *Tilburg Law Review, Journal of International and European Law*, 2015, 8; D. J. SOLOVE, *Nothing to Hide – the False Tradeoff between Privacy and Security*, New Haven, 2011, 24.

(GDPR),[5] the Court finds itself interpreting an innovative, though incomplete, legal framework. Therefore, the new regulatory framework codifies, also in the digital context, an evolving jurisprudence of the Court thanks to which the protection of personal data has taken different connotations over time to arrive today at a configuration oriented on fundamental rights. The historic *Stauder* judgment[6] of 1969 should be recalled as one of the first rulings in which the Court expressed its intention to protect the fundamental rights of the person, while respecting the aims of the then European Economic Community. In particular, the *Stauder* judgment concerned the right to privacy with regard to the processing of personal data. The Court of Justice further moved in this direction[7] in 1996, when Directive 95/46/EC (DPD),[8] – now replaced by the GDPR – came into force, as the Court found a more solid basis for its rulings in the Directive's provisions.

Initially, the case law of the Court placed the right to the protection of personal data in a dimension that was not autonomous yet, but at times functional and/or limiting, and certainly closely linked to the economic freedoms enshrined in the Treaties. This approach would gradually fade over time, under the influence of the case law of the Strasbourg Court on Article 8 of the EU Convention of Human Rights (ECHR) and on Convention No 108 of 1981, [9] which was also the subject of a revision process concluded on 18 May 2018 with the adoption of a modernization protocol by the Committee of Ministers.[10]

The evolution of the CJEU's case law on personal data would continue for several years in a substantially linear manner, until the adoption of Article 16 of the Treaty on the Functioning of the European Union (TFEU),[11] Article 39 of the Treaty of the European Union (TEU)[12] and

[5] 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, 1.

[6] Judgment of the Court of 12 November 1969, *Erich Stauder v City of Ulm – Sozialamt, Verwaltungsgericht Stuttgart – Germany*, 29/69, ECLI:EU:C:1969:57.

[7] See, among the others, the Judgments of the Court of 7 November 1975, *Adams*, 145/83, ECLI:EU:C:1985:448; of 26 June 1980, *National Panasonic*, 136/79, ECLI:EU:C:1980:169 and of 18 May 1982, *AM & S*, 155/79, ECLI:EU:C:1982:157,

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995, 31.

[9] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, European Treaty Series - No. 108, 1981.

[10] Modernised Convention for the *Protection of Individuals with Regard to the Processing of Personal Data*, 128th Session of the Committee of Ministers, CM/Inf(2018)15-final.

[11] "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

[12] "In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

the new Article 6 of the TEU.[13] Article 16 TFEU, in particular, brought the Court to deal with a new competence of the European Union in this area. Indeed, this article is not a simple reallocation of the old provision – Article 286 TEC (Treaty establishing the European Community) – nor it is limited to extending its application to the area of freedom, security and justice. Instead, Article 16 TFEU defines a Union competence concerning the protection of personal data, which decisively overcomes any doubt as to the scope of application of the secondary legislation adopted in this area.

On the other hand, the application of the EU rules on the processing of personal data is pervasive, since only few exceptions are allowed, namely for national security and for those activities which are exclusively personal or domestic in nature.[14]

In short, the Treaty of Lisbon ended up establishing a double safeguard of the right to the protection of personal data, creating a perfect contiguity between the Charter and the Treaties.[15] Article 8 of the Charter of Fundamental Rights[16] is the culmination of a codification process and *constitutionalization of the right to the protection of personal data* as built up in the case law, and at the same time it constitutes the cornerstone of the new legislative framework. With Article 8 of the Charter, from a dimension of essentially negative character – codified also by Article 7 of the Charter concerning the right to respect for private and family life[17] – the right to the protection of personal data leads to a positive dimension: Article 8 of the Charter establishes the existence of a new autonomous right. That said, this autonomy still struggles to emerge in the jurisprudence of the Court, even in the most recent cases. Indeed, the continuous reference to the right to respect for private and family life (Article 7 of the Charter) has caused some doubts on the nature and extension of the right to the protection of personal data, despite the undeniable adjacencies between these two rights. For example, in the *Promusicae* judgment[18] the Court affirms the existence of a new fundamental right, that is, the right that guarantees the protection of personal data and, therefore, of private life. However, as the Court of First Instance observed in *Bavarian Lager*,[19] "not all personal data are by their nature capable of undermining the private life of the person concerned".[20] Thus, the fundamental right to the protection of personal data should have a broader scope.

While it is true that the Court usually states in its rulings that Articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the Charter are closely linked to the point that they can be considered as forming part of a "right to privacy with regard to the

[13] "1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. (…)"

[14] Among these, the Court recently clarifies that the activity of door-to-door preaching of Jehovah's Witnesses should not be included (see Judgment of the Court of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551).

[15] Even if the Court always refers only to Article 8 of the Charter, the latter acts as an ideal link between other provisions of primary rank: Article 47 of the Charter, and Articles 4(3) and 19 of the TEU.

[16] Which, in paragraph 2, establishes the essential conditions for personal data to be processed.

[17] And by the ECHR in Article 8, as well as expression of the so-called "right" of the Union, is to be considered as a right of the European Union.

[18] Judgment of the Court of 29 January 2008, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54.

[19] Judgment of the Court of First Instance of 8 November 2007, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, T-194/04, ECLI:EU:T:2007:334.

[20] *Ibid*, para 119.

processing of personal data", the cumulative reference to these two rules seems to indicate the existence of a third right – independent of the other two. According to a different reading, the Court tends to use the general principles on data processing to give substance to the right to privacy, as the Strasbourg Court does by referring to Convention 108 of 1981.

In affirming the conceptual autonomy of the two rights, Advocate General Villalón, in his Opinion in the *Digital Rights Ireland* case,[21] argues that the link between them depends essentially on the nature of the data considered, since there are data that are, in a way, more than personal. According to his reasoning, the complexities begin already *upstream*, by the mere fact that circumstances relating to the most intimate sphere of a person have been able to crystallize in the form of data, that is in a form which may be subject to processing and for which, therefore, a reference to Article 7 of the Charter would also be justified. Therefore, it is a matter of a different positioning of the two fundamental rights. This could gradually lead to a functional separation between Article 7 and Article 8 of the Charter, which, in theory, should also allow for a stronger balance with other rights provided by the Charter.

The right to the protection of personal data, as the Court has pointed out in several judgments, is not an absolute prerogative either, but must be considered in the light of its social function. And the Court, in interpreting the rules of secondary law, has often found itself balancing the right to the protection of personal data with other fundamental rights. For example, the Court has given numerous judgments on the relationship between the protection of personal data, freedom of expression and the economic rights of operators.[22]

However, the balanced approach that the Court has always used in weighing the interests at stake must now be measured against the continuing advancement of technology. As mentioned, the digital world poses new challenges because it develops much faster than the law that should govern it, with the result that Courts are forced to appropriate the spheres of competence of the legislative power in an attempt to fill the gaps.

In this context, the judgment in *Google Spain* (C-131/123) [23] is emblematic and controversial. In such a case, the Court found reasons for the *right to be forgotten* to prevail over the public interest for easier access to information and over the economic rights of communication service providers, as well. Of course, this is not the case with freedom of expression and information, which, moreover, is one of the exceptions to the so-called *right to be forgotten* in the GDPR (see article 17).

It is no coincidence that, in the *Manni* judgment,[24] the Court gives precedence, in accordance with the principle of proportionality, to the purposes of legal disclosure over the needs of the individual, within a correct regulatory/exception relationship, in line with the case law of the Strasbourg Court.

The last – extremely delicate – aspect that should be analyzed is the apparent opposition between the right to the protection of personal data and the general interest to the security and

[21] Opinion of Advocate General Cruz Villalón delivered on 12 December 2013, *Digital Rights Ireland and Seitlinger and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2013:845.

[22] See, *ex multis*, Judgments of the Court of 6 November 2003, *Linvquist*, C-101/01, ECLI:EU:C:2003:596; of 24 November 2011, *Scarlet*, C-70/10, ECLI:EU:C:2011:771, of 16 February 2012, *SABAM*, C-360/10, ECLI:EU:C:2012:85; and of 16 December 2008, *Satamedia*, C-73/07, ECLI:EU:C:2008:72.

[23] Judgment of the Court of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

[24] Judgment of the Court of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.

prevention of crimes. In its judgment in *Digital Rights Ireland*,[25] the Court came to the conclusion that, although the core of the rights enshrined in Articles 7 and 8 of the Charter was not affected by the provisions of the Data Retention Directive (DRD),[26] the measures contained in the Directive were nevertheless disproportionate. This reasoning is also valid if the legislation of the Member States is scrutinized, as in the case of *Tele 2 Sverige*,[27] where the Court held that the minimum guarantees laid down by the *Digital Rights Ireland* judgment are imperative requirements of EU law – these guarantees being applicable, therefore, also to national regimes. Moreover, the mandatory nature of the standards laid down by the Court leads indirectly to review the compatibility of the legal systems of third countries with the system of protection of fundamental rights and freedoms laid down by EU law. This is, of course, a control which is carried out by way of mediation by the Commission which in fact implies a judgment of substantial equivalence, as in the *Schrems I*[28] and *Schrems II*[29] cases, or a decision with which an international agreement has been concluded. As for the latter, one could refer to the Court's Opinion 1/15 on the Passenger Name Record (PNR) agreement concluded by the European Union with Canada. In this way, the Court recognized an extraterritorial application of European standards for the protection of personal data. It is clear from this case law that any generalized and unconditional access by public authorities to personal data is incompatible with Articles 7 and 8 of the Charter, even if the purpose is to combat serious crime and regardless of whether the information relating to an individual's private life is sensitive or whether the person concerned has actually suffered negative consequences as a result of such interference. Thus, access to personal data by public authorities is permitted only if it is *targeted* and if the objective pursued by the rules governing such access are appropriate to the seriousness of the interference in fundamental rights. These are the terms with which the Court ruled *Ministerio fiscal*.[30]

The delicate balance between limitations of fundamental rights and security needs, therefore, is evaluated via a test of (strict) proportionality that allows the Court to enhance the centrality of the right to data protection and that, integrating the test of necessity, acts as a safeguard to defend the values of a democratic society.

At this stage, one might wonder to what extent the protection of personal data, with its physiognomy of fundamental right, can prevail not only over economic and social interests, but also over security requirements. The answer to this question is problematic because of the delicacy required in finding a balance between these interests. The protection of personal data is not only an individual right, but also a public interest, a guarantee for democratic life and, therefore, for the values on which the Union is founded. At the same time, security is not only

[25] Judgment of the Court of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

[26] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 *on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, OJ L 105, 13.4.2006, 54 (no longer in force).

[27] Judgment of the Court of 21 December 2016, T*ele2 Sverige*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

[28] Judgment of the Court of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, C-498/16, ECLI:EU:C:2018:37.

[29] Judgment of the Court of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

[30] Judgment of the Court of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788.

a public good, but also an individual right and a primary human need – arguably a decisive force behind the formation of our communities. One of the largest of these communities is now the European Union, which has an obligation toward our security, even of a positive nature. On the other hand, Article 6 of the Charter tells us that everyone has the right to liberty and security, even though the meaning of the latter expression, which is difficult to be recognized as an autonomous right, is still undefined in the case law of the Court. In short, the relationship between the protection of personal data and security should not necessarily be seen in an antinomic dimension.

Therefore, the constitutionalization of the right to data protection still leaves a lot of uncertainties when it comes to the balance between the data protection right and further fundamental rights. One should note that the GDPR itself,[31] which clearly promotes the fundamental right to data protection, recognizes that we should not regard the latter as an absolute right, since its role in society and its relationship with other fundamentals rights should find a balance.[32] In this context, we believe that the EU system is still lacking a fully harmonized definition of the relevant conceptual categories, as well as harmonized mechanisms to balance the right to the protection of personal data and other fundamental rights.

2.1. The balancing act between the protection of data and their use in the public interest

In light of the COVID-19 pandemic, we consider important to quickly frame the need to balance public health concerns with the protection of personal data as a fundamental right. This is quite crucial in the debate concerning the so-called tracing apps, which allow for the identification of potentially risky interactions between users through the collection of their personal data.[33]

One thing seems certain: in the fight against COVID-19 these data help in stemming the spread of the virus and in saving lives. Therefore, any chosen solution has to deal somehow with data protection – a category that then find itself in a rather uncomfortable position.

International institutions, such as the Global Privacy Assembly,[34] the European Data Protection Board,[35] the Council of Europe[36] and national data protection authorities[37] have

[31] 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* (GDPR), OJ L 119, 4.5.2016, 1.

[32] Recital 4 GDPR.

[33] See L. MOEREL, C. PRINS, *Privacy for the homo digitalis, Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things*, SSRN, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 (last access 30 April 2020).

[34] See Global Privacy Assembly, *Statement by the GPA Executive Committee on the Coronavirus (COVID-19)*, 2020, https://globalprivacyassembly.org/gpaexco-covid19 (last access 30 April 2020).

[35] European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, 2020, https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en (last access 30 January 2021).

[36] Council of Europe, Joint Statement on the right to data protection in the context of the COVID-19 pandemic, 2020, https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter (last access 30 January 2021).

[37] For an overview of all the declarations of EU data protection authorities, see European Union Agency for Fundamental Rights, *Coronavirus pandemic in the EU - Fundamental Rights Implications* - Bulletin 1, Annex:

stated that data protection requirements ensure the safe and reliable collection and processing of data. With regard to the contact tracing mechanisms adopted by national governments in the fight against Covid-19, several national authorities and the European Data Protection Council reaffirmed that the rights recognized by the General Data Protection Regulation (under Article 23) may be limited in the event of extreme circumstances, such as a major health emergency.

All EU Data Protection Authorities (DPAs) have issued statements and/or opinions related to the Coronavirus pandemic, providing guidance to public authorities, employers and the media on how to support data protection standards in their efforts against COVID-19, reaffirming that *"health and data protection rights go hand in hand"*.[38] They also stress that any measure that would violate the rights to privacy and data protection should be based on the law and follow the principles of necessity and proportionality. Therefore, any tracing and related collection of personal data must pursue the sole purpose of reducing the dissemination of COVID-19 (purpose limitation) and personal data must be limited to the minimum necessary (data minimization).

Many of the DPAs statements coincided with the adoption of extraordinary measures or emergency acts, for example in Italy and Poland. In Italy, the European DPA issued an opinion on the first government decision to declare a six-month state of emergency, which included a provision on the collection and processing of personal data by civil protection authorities. In particular, the Italian data protection Authority (*Garante per la protezione dei dati personali*) stated that the Decision was in line with the rights and guarantees provided by the legislation and stressed that – at the end of the emergency – all public administrations involved in civil protection must ensure that data collected during the emergency are processed in accordance with normal procedures.

In this scenario, the tension between the protection of personal data and the safeguarding of health is evident. The set of rights granted by the GDPR seems to be a safe guide on how to devise a system for tracking individuals that respects both these interests – health and data protection. However, it seems clear that achieving such a balance puts both categories at risk. On the one hand, personal data are subject to unparalleled exposure and we cannot exclude that some countries may move towards models that run afoul of their GDPR obligations. On the other hand, health protection and the containment of the virus may be constrained by data protection requirements.

3. The definition of personal (and non-personal) data in the EU regulatory system

The second set of boundaries that this article intends to assess is the one between personal and non-personal data.[39]

In legal terms, there is nothing between personal data and non-personal data, and the two categories can be said to be mutually exhaustive. Moreover, in theory, it is hard to identify any kind of data as truly and permanently non-personal. One can, of course, distinguish categories

DPAs Statements on COVID-19, 44 ss., https://fra.europa.eu/en/publication/2020/covid19-rights-impact-april-1 (last access 30 January 2021).

[38] *Ibid*.

[39] On this profile, see also T. STREINZ, *The Evolution of European Data Law*, forthcoming in P. Craig and G. de Búrca (eds), *The Evolution of EU Law* (Oxford University Press, 3rd ed. 2021), chapter 29.

of non-personal data that are less likely to be qualified as personal data, such as environmental readings, spatial data, or data concerning industrial or agricultural activity.

In addition, as data are merged into data sets, their qualification as personal or non-personal data may change over time. Personal data sets may be anonymised, thus becoming non-personal data. On the contrary, non-personal data sets may be integrated with other data, or merged into even more complex data sets, thus allowing the identification of individuals. Given the ever-developing analytic capabilities, arguably almost any type of data can, at some point, be qualified as personal data, when merged and processed together with other data. Already in 1983, the German Constitutional Court recognised that, given the possibilities of automatic processing of data from various sources, it is difficult to qualify any type of data as truly irrelevant for the identification of natural persons, *i.e.*, not personal.[40]

Now, as mentioned in the introduction, it is crucial to try to delimit the non-personal data category so as to better understand its interactions with the personal data's one.

According to the Commission of the European Union,[41] *non-personal* data can be classified in two different ways with respect to their origin: data that from the outset do not concern an identified or identifiable natural person (such as weather data); data that were initially personal and only later became anonymous through a process of anonymization (*e.g.* data concerning the travel abroad of a person after the use of special techniques to ensure anonymity).

However, the conditions under which data can be considered "anonymous" are controversial, with significant differences of opinion among the various institutions engaged in the development of European data protection law.[42] Moreover, the potential for re-identification has increased due to technological advances, making it "reasonably more likely" – as stated in recital 26 of the GDPR – that a natural person could become (re-)identifiable. In this context, the CJEU also does not provide us with a clear solution, as it has not yet addressed the anonymization of personal data.[43]

The difficulty of distinguishing between personal and non-personal data in theory and in practice, where mixed data sets containing both personal and non-personal data are extremely common, led some to argue that European data legislation should have dropped the binary distinction between personal and non-personal data in favor of a more holistic and differentiated regime. Nevertheless, the EU regulator has persisted in that direction.

Indeed, Articles 2 and 3 of Regulation (EU) 2018/1807 define as *non-personal data* all data other than personal data, referred to in Article 4(1) of Regulation (EU) 2016/679.[44]

---

[40] BVerfG Judgment of the Second Senate of 6 June 1983 – 2 BvR 209/83.

[41] Communication from the Commission to the European Parliament and the Council "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", COM(2019)250, para 2.1.

[42] See M. FINCK and F. PALLAS, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data under the GDPR*,10 *International Data Privacy Law*, 2020, 11.

[43] To date, the Court had to rule on relatively clear cases concerning the effort required to turn anonymous data into personal data. See Judgments of the Court of 16 February 2012, *Scarlet*, C-70/10, ECLI:EU:C:2011:771 (which held that a static IP address was personal data) and of 19 October 2016, *Patrick Breyer*, C-582/14, ECLI:EU:C:2016:779 (holding that a dynamic IP address was personal data if the Internet service provider could identify the person).

[44] I. GRAEF, R. GELLERT, N. PURTOVA, M. HUSOVEC, *Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data*, 2018, https://ssrn.com/abstract=3106791 (last access 31 January 2021).

Therefore, in order to identify the notion of non-personal data, it is not possible to disregard the General Data Protection Regulation, which defines *personal data* as: "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 specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[45]

Given the similarity with the definition already contained in the DPD (Directive 95/46/EC), it can be argued that, in accordance with what was observed by Advocate General Kokott in his conclusions in the *Nowak* case[46] the statement of personal data contained in the DPD has not been modified by the GDPR.[47] As a consequence, the specifications on the concept of *personal data*, elaborated by Opinion 4/2007 – also referred to as Working Document 136 (WP136),[48] by the Article 29 Working Party (WP29)[49] – remain significant sources even after the entry into force of the GDPR, although they are not binding and refer to the regulatory framework laid down by the DPD.

The same consideration can also be made for the rulings of the CJEU, which are therefore still to be considered fundamental for the definition of what is to be understood as *personal data* and, conversely, as *non-personal data*.

Over the years, both the WP29 and the jurisprudence of the CJEU identified four key elements that characterize the definition of *personal data*, namely the concepts of: any information; concerning; a natural person; identified or identifiable.[50] Since the notion of *non-personal data*, given by Regulation (EU) 2018/1807, is a mere negation of the one used for *personal data*, the same considerations made by WP29 and the CJEU for the individual components of one (personal data) can be used for the individual constituents of the other (non-personal data). Therefore, *non-personal data* should be understood as any information not relating to an identified or identifiable natural person, directly or indirectly.

However, the constituent elements of the definition are not undisputed. This will be briefly demonstrated also referring to decisions of the CJEU – that also in this case covered a leading role in the process.

In short, with regard to the first element – *any information* – neither Regulation (EU) 2018/1807, nor GDPR or the former DPD provide a definition of information. They merely

---

[45] Article 4(1), GDPR. This definition of "personal data" is not new in the European Union (EU) system. It is based on what had already been set out in Directive 95/46/EC (the "DPD"), in which the European legislator considered "personal data" "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity", Article 2, a), DPD.

[46] See Judgment of the Court of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994 and the Opinion of Advocate General Kokott, ECLI:EU:C:2017:582, para 3.

[47] See N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, *Law, Innovation and Technology* 2018, 10(1), https://ssrn.com/abstract=3036355 (last access 31 January 2021).

[48] Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136 (hereinafter "WP136").

[49] The EU's advisory body on data protection until November 2016.

[50] I. GRAEF, R. GELLERT and M. HUSOVEC, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation*, TILEC *Discussion Paper* 2018-029, https://ssrn.com/abstract=3256189 (last access 31 January 2021).

determine the meaning of data, whether personal or not, sometimes also by using the terms information/data interchangeably in the same context[51] as, for example, in recital 26 of the DPD.[52]

Moreover, the Working Party only points out the clear will of the European legislator to give a broad formulation of personal data,[53] and then specifies that any information, by its nature, content or format, can be identified as personal data.

Similarly, the CJEU in the *Nowak* case,[54] with regard to the meaning of *any information*, has established: "The use of the expression 'any information' in the definition of the concept of 'personal data', within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject".[55]

Moving on to the second element – *the possibility that information may or may not be related to an identified or identifiable natural person, directly or indirectly* – the WP29 noted that sometimes the relationship between physical subject and information can be easily identified, as in the case of the image of a person who is filmed during an interview or the medical record of a particular subject. Other times, however, it is more complex, as in the case in which information is related to objects, because only indirectly it can be claimed that these are related to individuals. As an example, the value of a house (object) is identifiable as personal data when "will hence be used to determine the extent of this person's obligation to pay some taxes" [56] and, therefore, only indirectly connects to the natural person. As a conclusion, WP29 specifies that "in order to consider that the data "relate" to an individual, a "content" element or a "purpose" element or a "result" element should be present."[57]

In this context, the case law of the CJEU has evolved. In 2013, the Court, ruling on the joined cases *YS and M, S*[58] with regard to access to minutes concerning the temporary residence permit as a right of asylum in the Netherlands, argued that although there was no doubt that the minute included personal data, it could not be identified on the basis of its content, as it did not constitute personal data within the meaning of the DPD.[59] In fact, based on the conclusions of Advocate General Sharpston, the CJEU noted that "such a legal analysis is not information relating to the applicant for a residence permit, but at most, in so far as it is not limited to a purely abstract interpretation of the law, is information about the assessment and application by

---

[51] See W. G. URGESSA, *The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging 'Data' as Exclusively Informational*, in *Journal of Intellectual Property, 7 Information Technology and Electronic Commerce Law*, 2016.

[52] Which reads: "*the principles of protection must apply to any information concerning an identified or identifiable person* […] *but the principles of protection do not apply to data* […] *rendered anonymous and retained in a form in which identification of the data subject is no longer possible*".

[53] WP136 cit., 6.

[54] Judgment of the Court of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994.

[55] *Ibid*., para 34.

[56] WP136 cit., 10.

[57] *Ibid*., 10.

[58] Judgment of the Court of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel*, C-141/12, ECLI:EU:C:2014:2081, para 18.

[59] *Ibid*., para 38 and 39.

the competent authority of that law to the applicant's situation, that situation being established *inter alia* by means of the personal data relating to him which that authority has available to it".[60]

Consequently, the Court prevented the exercise of the right of access provided by Article 12 of the DPD, since the legal analysis at hand was not to be regarded as falling within the definition of personal data. The CJEU has therefore interpreted the concept of "concerning" in the *YS, M and S* cases in a restrictive sense, without referring to the WP29.

Indeed, while in WP136 the "content" concerning the person may be the most varied, for the Court, even if the document itself contains personal data, it does not imply that such information must be related to a natural person. As stated, indeed, the reference to an individual is to be excluded if the information concerns the assessment and application of the right by the authority to a situation defined through personal data. Compared to Opinion 4/2007, there is also a lack of mention of the purpose or outcome of the collection of information, which has not been examined by the CJEU, leaving WP136 the only document referring to these alternative criteria for verifying the existence of the "concerning" element.

However, the CJEU has subsequently changed the mentioned jurisprudential orientation.[61] In particular, in the *Nowak* decision the Court, with regard to the "concerning" parameter, stated that: "it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person".[62]

In the CJEU's reasoning, the influence drawn from WP136 is clear, as is the diversity with what was stated in the *YS, M and S* cases. In fact, while in 2014 the Court had adopted a restrictive view of the concept of "concerning" (to the extent that it did not encompass an authority document that included personal data under the protection of the DPD because it did not relate to the individual), in 2017, with the *Nowak* case it accepted a broad interpretation of the "concerning" element, in line with the reading provided by the WP29.

The decision on the right of access is also different. While in *YS, M and S* the Court had denied the protection of the right to a private life by giving access to a document that was not personal data, in *Nowak* the CJEU argues the exact opposite: giving a candidate access to the examination answers and comments "serves the purpose (…) of guaranteeing the protection of that candidate's right to privacy with regard to the processing of data relating to him."[63]

Ultimately, The *Nowak* case limits the restrictive scope of the previous *YS, M and S* ruling and allows for a broader interpretation of the "concerning" element in accordance with the WP29.[64] This makes it easier to identify any information as personal data and, conversely, makes it more difficult to identify it as non-personal data.

[60] *Ibid*., para 40.

[61] Following the claimant's request for access to the failed examination tests, the Supreme Court of Ireland had asked the CJEU, *inter alia*, whether the answers to the questions in the assessments constituted personal data within the meaning of Article 2(a) Directive 95/46/EC. The CJEU's reply was positive.

[62] Judgment of the Court of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, para 35.

[63] *Ibid*., para 56.

[64] *Ibid*., para 7.

Now, focusing on the third element, the *concept of a natural person* – one should note that it is described in Article 6 of the Declaration of Human Rights, [65] which states that "Everyone has the right to recognition everywhere as a person before the law".

The WP29 addresses in this regard three orders of problems that – although they will not be the specific focus of this article – allow us to highlight once again the many interpretative complexities that still exist, despite the adoption of the GDPR, which clarifies them only in part. They are the application of the protection of personal data to data relating to the deceased, the unborn child and the legal persons. In short, legal persons are not always exempt from the discipline of personal data protection; the issue of the unborn child has not yet been normatively resolved at European level (but could be specified by national policies with internal regulations), while the issue of data on deceased natural persons has been addressed by the GDPR, but in practice still has a problematic relevance. With regard to the application of data protection concerning a legal person, in general, the application of the GDPR can be excluded as it applies only to "natural persons". However, the CJEU clarified that information relating to sole proprietorships may constitute personal data if it permits the identification of a natural person.[66]

Assessing the last and fourth aspect – *i.e.*, *identified* – we can first rely on the interpretation of the WP29 which considers the case of a person who, in a group, is distinct from all others.[67] On the other hand, "*identifiable*" means a person who can be identified, even though he or she has not yet been identified in a multitude. According to the GDPR and, before, the DPD, one becomes identifiable in two ways – either directly or indirectly. [68] For identification purposes, recital 26 of the GDPR[69] determines the assessment of "all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly".[70]

The WP29 then specifies that this weighting must take into account the factors at stake, such as "the intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organizational dysfunctions (e.g. breaches of confidentiality duties) and technical failures (…)".

The Working Group 29 also states that the means of identification have a dynamic nature. As a consequence, in order to address the test of reasonableness in an adequate manner, one has to "consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed".[71] For this reason, the fact that at a specific point in time identification is not possible does not preclude that in the future, as technological processes advance, it will be.[72]

---

[65] WP136 cit., 22.

[66] In *Worten* Case, the CJEU stated that data contained in a register of working time of a company should be considered "personal data" since they are information concerning an identified or identifiable person, see Judgment of the Court of 30 May 2013, *Worten v Authority for Employment Conditions*, C-342/12, ECLI:EU:C:2013:355, para 35.

[67] WP136 cit., 12.

[68] Article 2 letter a) Directive 95/46/EC and Article 4 GDPR.

[69] See Recital 26 Directive 95/46/EC.

[70] Similarly, Working Party 29 Opinion 4/2007 follows the same concept of reasonableness, pointing out that "the mere hypothetical possibility of distinguishing a person is not enough to consider him or her 'identifiable'".

[71] *Ibid*., 15.

[72] For example, the Court pointed out that the Internet Protocol (IP) addresses of the individual websites, accessible thanks to the service offered by Scarlet constitute protected personal data, as they allow the precise identification of users. The criterion of identifiability was therefore used in these proceedings to affirm that

The Court – in *Breyer*[73] – then clarified that it is not necessary "that all the information enabling the identification of the data subject must be in the hands of one person".[74] This decision is relevant because it allows the individuation of a subject also through the combination of quantity of information coming from different data controllers, widening the possibility of recognizing the individual, above all with respect to the exponential growth of data collected in recent years.

Having considered one by one the components of the definition of personal data, from which the meaning of non-personal data derives, it is necessary to address the actual distinction between personal and non-personal data.

Adopting the concept of "any information" expressed by WP29, and confirmed by the CJEU in the *Nowak* case, there would remain few things not to be considered as falling into the category of data (*e.g.*, human samples). Almost everything could be data, to be submitted either to the subcategory of personal data or to the subcategory of non-personal data.

The discriminants between the two categories (personal and non-personal data) are the other three elements, namely the notions of: concerning; a natural person; identified or identifiable. Therefore, if an information does not concern an identified or identifiable natural person, it is non-personal data. In order to satisfy such a requirement, both the WP29 and the CJEU (after the *Nowak* case) consider that the information should not be related to a natural person identified or identifiable (to be assessed according to the index of reasonableness of the means used for the identification). In particular, the information should *not* be related to a natural person by means of its content, the purpose with which it was collected, or the result that its processing involves.

Among the listed criteria, the element of being identifiable is particularly critical and worthy of further investigation. In fact, as highlighted by the CJEU in the *Breyer* case, a person can also be identified by cross-referencing information from different data controllers. In practice, therefore, a website operator who is unable to identify, for example, an individual who visited its webpage with the information collected through its page alone, could actually identify this person by gathering additional information provided by another internet provider.

In addition, WP29 highlights the dynamic nature of the identification process, as it is subject to technological development. Thus, if today a piece of information does not appear related to an identifiable person because it is not possible to identify that person, tomorrow a technological development might enable that.

---

information (the visit to a website) related to a natural person (the user), constitutes "personal data" because the individual was identifiable by means of the IP address, linked to the webpage in a collection that had been made by Internet access provider; see Judgment of the Court of 24 November 2011, *Scarlet*, C-70/10, ECLI:EU:C:2011:771. In *Breyer*, the Court then ruled on dynamic IP addresses – that is assigned to each connection to the internet and replaced in the event of subsequent connections – do not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer. However, it was necessary to verify whether the person could have been identified indirectly, through the use of means that could reasonably be used by the controller or others; see Judgment of the Court of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, para 38 ss.

[73] See F. ZUIDERVEEN BORGESIUS, *Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition (Case Note), 3 European Data Protection Law Review*, 2017, https://ssrn.com/abstract=2933781 (last access 31 January 2021).

[74] Judgment of the Court of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, para 43.

Therefore, it seems evident that – on the one hand – the category of personal data has grown exponentially and that – on the other hand – there are numerous difficulties in interpreting the limits between personal and non-personal data.

This is even more relevant if one considers that Regulation (EU) 2018/1807 on a framework for the free movement of non-personal data within the European Union[75] only applies to data other than personal data. As a consequence, in the event of a mixed set of data (that is, composed of both personal and non-personal data), such Regulation will be applied only to the part of the information that does not concern an identified or identifiable natural person, while the GDPR will apply to the remaining part of the information, which can be classified in the category of personal data.

Moreover, the GDPR for sure prevails in cases where it is difficult to discern the two categories of data and their provisions. Indeed, Article 2, paragraph 2 of the Regulation 2018/1807 provides that, in the event that personal and non-personal data should be "inextricably linked", the application of the GDPR is not affected.

In summary, with the recent regulations relating to personal and non-personal data, the legislator established a system of cross-references between the two regulations that may hinder compliance.

4. Conclusions

In light of the analysis carried out in the article, we can argue that the category of personal data in the European Union broadened in its scope and relevance thanks to both the activity of the CJEU and the EU regulator. On the one hand, this expansion responds to a welcomed and growing interest in protecting individuals; on the other hand, the dual path of analysis taken in this article allows us to identify areas where we believe that a clarifying intervention by the Court of Justice is necessary.

Concerning the nature of fundamental right of the personal data protection, we have stressed that many uncertainties remain with regard to the balance between the protection of personal data and other fundamental rights (paragraph 2 above).

The actual implications of these uncertainties are numerous. One could think about the general public interest of not overly slowing down the development of the digital economy, in light of fundamental rights connected to the collection and processing of personal data.

Another crucial implication occurs if we consider the need to balance public health concerns with the protection of personal data as a fundamental right – in light of the Covid-19 pandemic. In this direction, we borrow from "Privacy 2030: A Vision for Europe", based on Giovanni Buttarelli's vision: "Personal data can and should be used to serve the public interest, the general interests of state and society rather than those that benefit distinct groups or individuals".[76]

A solution to such a lack of harmonization could be in the activity of the CJEU. Indeed, with its jurisprudence, the Court could bring back the fundamental right to the protection of

[75] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018, *on a framework for the free flow of non-personal data in the European Union*, OJ L 303, 28.11.2018, 59.

[76] See C. D'CUNHA, *Privacy 2030, A New Vision for Europe, Based on Giovanni Buttarelli's vision*, 2019, https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf (last access 31 January 2021).

personal data to its appropriate dimension, without yielding to the temptation to grant it an absolute acronychal and impermeable value, but equally aware that, by now, it is configured as an indispensable constitutional garrison and also one of the highest points of the process of European integration.

Regarding the boundaries between personal and non-personal data, the scope of the first category seems to increase more and more in broadness and the existence of a dataset free of personal data appears to be configurable in extremely rare circumstances. In particular, whenever personal data are not perfectly discernible from non-personal data, then the GDPR will necessarily apply and, as a consequence, compliance costs with regard to mixed datasets (which are more widespread) will rise. As a consequence, data-driven companies risk having to comply with the data protection regulatory framework for an entire dataset – even in its non-personal data component. Also in this context, we believe that it would be desirable to involve the Court of Justice in better clarifying the boundaries of the category of non-personal data in positive terms and in understanding the process of anonymization of personal data.[77]

[77] As mentioned above, to date, the Court had to rule on relatively clear cases concerning the effort required to turn anonymous data into personal data. See Judgments of the Court of 24 November 2011, *Scarlet*, C-70/10, ECLI:EU:C:2011:771 and of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.