CHAPTER ONE

GDPR and the Right to Personal Data and Privacy in a Modern Society in the Digital Age

SOŇA MATOCHOVÁ

1. Introduction

It is not going too far to say that the tension between data use and data protection is one of the defining features of the new millennium,[1] also known as the digital age. The protection of personal data and privacy in the context of advanced technological developments and globalisation requires both robust and coherent legal framework that allows individuals to control their own data. In this context, this Chapter addresses questions connected with current European data protection legal framework, e.g. whether the General Data Protection Regulation (GDPR)[2] is successful in practise, what are its problems, specific features and shortcomings and whether there are reasons to reconsider the valid legal framework, either substantially or partially. Although this chapter deals mostly with theoretical issues, it does not neglect practical needs.[3] The red line followed in this contribution are both the special characteristics of the fundamental right to data protection and the assessment of the nature and effectiveness of the current data protection framework. The topic which has been chosen for this collection of contributions focusing on European law issues is highly up to date, containing open questions on the relationship between technology and

[1] Paul Craig a Gráinne de Búrca. Series Editors Preface. In LYNSKEY, O. *The foundations of EU data protection law.* First edition. Oxford, United Kingdom: Oxford University Press, 2015. xxiv, 307 pages. Oxford studies in European law. ISBN: 9780198718239.

[2] 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).

[3] The author of this article has been analysing personal data protection issues in individual areas of data processing at the Czech data protection supervisory authority for the last seven years, using her previous professional experience in constitutional law and European law.

personal data, which need to be seen from the perspective of legal (including constitutional) and ethical aspects. However, current data processing issues, i.e. questions of personal data in the context of technology development, are often interdisciplinary and complex. Over that, they are closely linked to human rights, democracy and the rule of law, such as the question of surveillance of citizens through technology means.[4]

The framework described above is the reason why the application and interpretation of the fundamental right to data protection could be described as demanding and challenging for the responsible actors (controllers, supervisory authorities, national courts, data subjects, Internet service providers) from a practical point of view, moreover, information and communication technologies are evolving exponentially, while some complex data processing questions are answered by supervisory authorities or by courts gradually and over a long period of time. Data controllers often do not take a comprehensive view of data processing issues from the perspective of the GDPR layered approach, and as a result, they are unable to apply the GDPR principles properly, which leads to formal application of GDPR. Generally, the GDPR requires the qualified application of its general principles in relation to the specific data processing, which presumes not only knowledge of both data protection legal framework and expert fields relating to specific processing (e.g. AML[5] or whistleblowing), but also at least basic understanding of technologies used for data processing. The question for data controllers is how to apply adequately the abstract GDPR principles, if the are to be protected really and effectively, not only formally. It can be noted that only a limited number of data protection authors and commentaries[6] are focusing on specific features of the fundamental right to data protection, most authors limit themselves to state that the right to data protection is a fundamental right. Nevertheless, the understanding to the constitutional dimension of the right to data protection in relation to specific processing[7] poses a challenging and difficult task for data controllers.

---

4 The term technology in the context of this article means any current advanced technological solution in the online environment based on the processing of data, including personal data.

5 AML is used as an abbreviation for anti-money laundering.

6 LYNSKEY, O. *The foundations of EU data protection law.* First edition. Oxford, United Kingdom: Oxford University Press, 2015. xxiv, 307 pp. Oxford studies in European law. ISBN: 9780198718239.
GONZÁLEZ FUSTER, G. *The emergence of personal data protection as a fundamental right of the EU.* Cham: Springer, 2014. xvi, 274 pp. Law governance and technology series, 16. ISBN. 978-3-319-05022-5.
KUNER, Ch. (ed.)., BYGRAVE, L. A. (ed.)., DOCKSEY, Ch. (ed.)., DRECHSLER, L. (ed.). *The EU General Data Protection Regulation (GDPR): a commentary.* First edition. Oxford, New York: Oxford University Press, 2020. ISBN: 9780198826491.

7 Constitutional jurisprudence sometimes uses the term *shining constitutionally protected values into ordinary (simple) law* for explanation of the constitutional law influence in the legal order.

In the area of data protection, there are a number of issues where to reach compliance with the GDPR rules is a difficult task. The risk to the rights and freedoms of natural persons may result from personal data processing which could lead to physical, material or non-material damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage.[8] Another example could be when some controllers who process large volumes of data including personal data in connection with services offered by them try to use the collected data, without the consent of data subject, for purposes other than those for which the data was originally collected.[9] In some cases, controllers argue that they have anonymised the data so that they are not processing personal data. However, according to current scientific knowledge it is technically difficult to anonymise personal data in order that they could not be retrospectively de-anonymised, i.e. linked to an original identifiable person. Recently, the so-called Stanford study addressed the issue of de-anonymisation of web browsing data on social networks, concluding that a full 72 % of the data can be linked back to identified or identifiable natural persons, so they are not longer anonymised data.[10] As for another example, there are also different views on the prohibition of data monetisation, although people usually take the view that personal data are not tradable. Also, there are references in European law that the right to data protection as a fundamental right implies that personal data is not a tradable commodity.[11] The task of data protection law and practise is precisely to find answers to such complex questions.

2. The relationship between data protection and privacy in EU law in the digital age

The tension between the free use of data and the protection of personal data has been reflected in Europe since the 1970s, which contributed to evolution

See also judgment of the Constitutional Court of the Czech Republic III. ÚS 139/98.

8 Point 75 GDPR.

9 Point 50 GDPR Preamble.

10 De-anonymising web browsing Data with Social Network. Jessica Su. Sharad Goel. Stanford University. Available at: https://dl.acm.org/doi/pdf/10.1145/3038912.3052714.

11 European Commission. Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalized World. Brussels, 10 January 2017. *Respecting privacy is a condition for stable, secure and competitive global commercial flows. Privacy is not a commodity to be traded*.

of personal data protection independence.[12] From that time it was clear that for situations of large-scale processing of individual's data, which can in principle be collected, disclosed, copied, processed and replicated without restriction, privacy protection measures are not sufficient. The relationship between the two rights, i. e. privacy and personal data, has gradually evolved and refined against the background of rapid technological development, as reflected by milestones of legal data protection, which are above all the Council of Europe Convention 108 of 1981[13] and later on, Directive 95/46/EC,[14] both of which were based on personal data and privacy protection. While initially the right to data protection was "overshadowed" by the right to privacy, it has become gradually fully emancipated. In EU law, unlike the European Convention on Human Rights,[15] both the right to data protection and the right to privacy are separate fundamental rights regulated by the EU Charter of Fundamental Rights and Freedoms (the EU Charter).[16] Nevertheless, both in practice and in theory these two rights are often not distinguished, they are confused or the right to data protection is considered as part of the right to privacy. There is useful to define their relationship at the outset of described topic clarification.

In general, the right to data protection and to privacy are closely linked and both of them can contribute to protect the values of privacy and integrity of individuals. Nevertheless, these rights are different in terms of their rationale and content. The fact that both rights are independent is also clear from the text of the EU Charter of Fundamental Rights which regulates them separately from 2009. Even during legislative work on the GDPR draft, all references to privacy had been consistently removed from the text. It can be stressed that the EU law has not only enshrined the above two rights by means of different and separate provisions of the EU Charter,[17] but they differ both in terms of their systematic classification, and in terms of data protection exercise and enforcement before relevant authorities and courts. Despite the different procedures,

[12] The concept of personal data first appeared in the 1960s.

[13] Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data in the wording of its Protocols and Amendments.

[14] 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.

[15] Both the European Convention of Human Rights and the US law are based on the right to privacy.

[16] Charter of Fundamental Rights of the EU. Official Journal of the European Union. 2012/C 326/02.

[17] This is not the case in the Convention for the Protection of Fundamental Rights and Freedoms, which only guarantees the right to privacy. Nor is it the rule that all EU Member States' constitutional orders enshrine both rights.

the enforcement of both rights can contribute to the protection of private space of individual.

For the reasons given above, it is not systematically correct to state that the right to data protection is part of the right to privacy, or *vice versa*, as the relationship between the rights concerned is complex and multi-layered, they can overlap or complement each other in their operation depending on the specific situation, or they may not apply to the concerned situation at all.[18] In some situations, data protection measures may directly or indirectly contribute to the protection of an individual's privacy both as a consequence of general concept and broad interpretation of the right to data protection, which has been repeatedly confirmed by the Court of Justice of the EU (CJEU).[19] This broad concept of data subjects' rights in the GDPR, specifically, for example, the right of access to personal data, the right to be forgotten or the right to rectification, can effectively help to protect privacy.[20] In addition, data protection tools can effectively play a preventive role *pro future* provided the controller remedy the identified deficiency. Often, data protection remedies are in practice more enforceable and effective from the perspective of the individual, whereas privacy remedies pursued through legal actions before the courts could be lengthy and their outcome uncertain. The intertwining of the value of privacy and personal data protection may also partly overcome the division between private and public law, due to the fact that each of these rights may be broader or narrower in relation to the other. On the other hand, the protection of personal data and privacy are often referred to as a single concept, without distinguishing between them, which in principle cannot be objected when speaking generally, but also in view of the broader human rights concept described in the European Court for Human Rights (ECHR) case law, which does not distinguish between the above two rights. On the other hand, precise terminology is necessary when speaking about specific

[18] GELLERT, R., GUTWIRTH, S. The legal construction of privacy and data protection. *Computer Law & Security Review (CLSR).* 2013, vol. 29, 522–530 (ISSN 0267-3649). *All in all, data protection and privacy overlap on a mode whereby data protection is both broader and narrower than privacy. It is narrower because it only deals with the processing personal data, whereas the scope of privacy is wider. It is broader, however, because it applies to the processing of personal data, even if the latter does not infringe upon privacy. Privacy is also broader and narrower: it might apply to a processing of data which are not personal but nevertheless affects one's privacy, while it will not apply upon a processing of personal data which is not considered to infringe upon one's privacy. It can be said as well that a processing of personal data can have consequences not only in terms of privacy, but also in terms of other constitutional rights, and most obviously, when the processing of data relating to individuals bears risks in terms of discrimination.*

[19] CJEU judgment C-293/12 Digital Rights Ireland of 8 April 2014. Point 48.

[20] EDPB Guidelines 1/2022 on data subject rights – right of access of 28 March 2023. Version 2. Point 13. The controller cannot deny the access of data subject to the data which he/she is going to use before court.

legal protection in a particular case. Of course, both rights are executed and enforced quite differently.

The above-mentioned relationship between the right to privacy and the protection of personal data, consisting in their interdependence with ethical values and requirements of the dignity and autonomy of the individual guaranteed in the constitutional order, was precisely expressed by the data protection expert Peter Hustinx[21] when he stated: *"Privacy and data protection – more precisely: the right to respect for private life and the right to the protection of one's personal data –are both fairly recent expressions of a universal idea with quite strong ethical dimensions: the dignity, autonomy and unique value of every human being. This also implies the right of every individual to develop their own personality and to have a fair say on matters that may have a direct impact on them. It explains two features that frequently appear in this context: the need to prevent undue interference in private matters, and the need to ensure adequate control for individuals over matters that may affect them."*[22] This broader perspective highlights the complexity and interdisciplinarity of the categories of data protection and privacy, which also have ethical and constitutional dimension.

3. The right to the protection of personal data as a fundamental right

The fact that the right to data protection is enshrined as a fundamental right in the EU Charter means that it has a privileged (stronger) position within the legal order than ordinary rights, so it is more difficult to limit it or interfere with it (but this is not excluded as it is not an absolute right). In order to limit the right to data protection, it is necessary to apply the step-by-step assessment (methodology) generally used to assess limitations or conflicts between fundamental rights. This mechanism is provided for in Article 52 (1) of the EU Charter. The fact that the right to data protection is a fundamental right finds its expression in the application and interpretation of this right, both at EU and national law level. The proper application and interpretation of the data protection right by the obliged entities is facilitated by the fact that the various aspects of the data protection law framework are interpreted both by the European Data Protection Board (EDBP) and, above all, by the case law of the CJEU, or the case law of ECHR, where applicable.

[21] Peter Johan Hustinx (born 1945) is a Dutch lawyer who served as European Data Protection Supervisor (EDPS) from January 2004–2014.

[22] Available at: https://edps.europa.eu/sites/edp/files/publication/14-09-08_article_uji_castellon_en.pdf.

The protection of natural persons with regard to the processing of personal data as a fundamental right is enshrined both in Article 8 (1) of the EU Charter of Fundamental Rights of the European Union (hereinafter referred to as the EU Charter) and Article 16 (1) of the Treaty on the Functioning of the European Union (hereinafter referred to as the TFEU), which grant everyone the right to the protection of personal data concerning them. *See Table: Relevant legislation in the field of personal data.* Article 8 of the EU Charter is specific in terms of its wording, structure and content compared to the other rights regulated by the EU Charter. The right to the protection of personal data not only guarantees, but also sets out (specifies) in its Article 8 (2) the conditions for the processing of personal data, which means the correct processing of data, the existence of purpose, the existence of a legal basis for the processing, the guarantee of the right of access to collected personal data and the right to rectification. Article 8 also requires, in paragraph 3, supervision by an independent authority controlling compliance with data protection rules.[23] This way of constructing the right to the protection of personal data in the EU Charter, chosen by the European law-maker in Article 8 of the EU Charter, is specific compared to other rights as in terms of the fact that it describes relatively precisely the content and limits of this right. However, it is clear that the wording pursues a realistic setting of the right to data protection in the form of a data quality requirements of the personal data processing,[24] including the institutional guarantee of supervisory data protection independent authority.

The wording of the right to data protection in the EU Charter is further specified by the GDPR, according to which the right to data protection is not an absolute right; it must be considered in the context of its function in society and, in accordance with the principle of proportionality, it must be balanced with other fundamental rights. The GDPR mentions that it respects all fundamental rights and observes the freedoms and principles recognised by the Charter as enshrined in the Treaties, in particular respect for private and family life, home and communication, protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom of establishment, the right to an effective remedy and to a fair trial, as well as cultural, religious and linguistic diversity.[25] Although the GDPR does not explicitly mention the value of human dignity in the above demonstrative list, it is undoubtedly an essential requirement and an integral part of the right to data protection, which can be significantly affected by the processing of personal data, for example, in the form of

[23] Art. 8(3) EU Charter. Compliance with these rules shall be subject to control by an independent authority.

[24] Art. 8(2) EU Charter contains only some of GDPR principles.

[25] Point 4 GDPR Preamble.

an individual's feeling that he or she is under constant surveillance. The conflict between different rights must always be assessed both according to the nature of rights at stake and the specific circumstances of the processing in question. In practice, this means first to identify the rights and interests that may potentially be affected by the processing. In this respect, personal data processing records are used.[26] In case of some processing, data protection impact assessment (DPA) is obligatory.[27] By the way, the DPA is extremely useful even in situations where the GDPR does not explicitly impose such an obligation on the controller.[28] The balancing of the right to data protection with other (fundamental) rights is realised by applying the proportionality principle based on Article 52 (1) of the EU Charter.[29]

The complex system of assessing the fundamental right to data protection in the EU on multiple levels also reflects the default setting of the GDPR, which envisages both the freedom of data flow and the protection of personal data. This approach emphasising both rights is sometimes referred to as the rights-based approach.[30] The two, in relation to the specific processing contradictory values, pursue quite different goals. While the rationale for enshrining the free movement of data was for the EU states to be able to benefit from the economic and other societal benefits that data processing technologies can potentially bring, including, for example, the exploitation of big data phenomenon, on the other hand side, individuals cannot be deprived of their space of freedom and privacy which has been traditionally recognised in various forms, such as the right to privacy, the right to be left alone, the right to informational self-determination or the right to data protection. These rights are expression of the individual's need to have a certain personal space in which they can develop freely without the supervision of others.[31] From this perspective, collection of personal data by technologies, which in principle can be replicated and disseminated without

[26] Art. 30 GDPR.

[27] Art. 35 GDPR.

[28] Art. 35 GDPR. Guidelines on Data Protection Impact Assesment (DPIA) and determining whether processing is likely to result in high risk for the purposes of Regulation 2016/679/EU. WP 248 rev.01.

[29] The Constitutional Court of the Czech Republic has expressed its opinion on this issue in its judgment Pl. ÚS 37/17 when it stated: The Constitutional Court in its established case law requires that in the event of a conflict between fundamental rights or freedoms and public interest or other fundamental rights or freedoms, the purpose (objective) of the intervention must be assessed in relation to the means used, with the principle of proportionality being the benchmark of the assessment.

[30] LYNSKEY, O. *The foundations of EU data protection law.* First edition. Oxford, United Kingdom: Oxford University Press, 2015, xxiv, 307 pp. Oxford studies in European law. ISBN: 9780198718239.

[31] It is claimed that the first mention of privacy in literature can be found in the 1890 article The Right to Privacy by S. D. Warren and L. D. Brandeis. See WARREN, S. D., BRANDEIS, L. D. The Right to Privacy. *Harward Law Review*. 4/1890, no. 5, pp. 193–220.

restrictions, is a massive invasion to personal data and privacy. Therefore, such collection of data should not occur in an arbitrary and purposeless manner. From an ethical perspective, processing of personal data should serve people[32] in the form of some desirable purpose, social good or interest. Accordingly, the EU legal framework for data protection implies that, while the free flow of data must be preserved, there should be no arbitrary, excessive or unnecessary processing of personal data (the principles of the GDPR in Articles 5 and 6 and other provisions serve to prevent such processing). These requirements apply throughout the Union and ensure a consistent and uniform application of the rules on the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data.[33]

4. Limitation of the fundamental right to the protection of personal data in the EU

As already mentioned, the data protection legal framework enshrines the right to the protection of personal data as a fundamental right, but at the same time provides that it is not an absolute right and foresees that it can be limited. Such restriction must follow the requirements set out for fundamental rights in Article 52 (1) of the EU Charter. In this spirit, the CJEU also explicitly states that the justification for the interference with the rights guaranteed by Articles 7 and 8 of the EU Charter must be made on the basis of Article 52 (1) of the EU Charter. This Article sets out several cumulative conditions: any restriction on the exercise of the rights and freedoms enshrined in the EU Charter must be provided for by law (1), respect the essence of the rights at stake (2) and, subject to the principle of proportionality (3), restrictions on those rights and freedoms may only be imposed if they are necessary (4) and if they genuinely meet objectives of general interest recognised by the Union or the need for the rights and freedoms of another (5).[34] Each of these abstract requirements set out in Article 52 (1) must be assessed separately and with due care, while the controller does not have absolute certain about the correctness of his/her assessments (based on GDPR requirements and principles). In any case, the assessment of conditions is the responsibility of the controller.[35] These requirements include the principle of necessity, which provides that restrictions may be imposed only if they are necessary, and the principle of proportionality, which is a tool for striking a balance

[32] Point 4 GDPR Preamble.
[33] Point 10 GDPR Preamble.
[34] Art. 52(1) of the EU Charter.
[35] Art. 24 GDPR.

with other rights. The requirement of proportionality can be found in the GDPR not only for balancing competing rights, but also as a general principle applied by the controller in relation to the application of the various measures of the GDPR (e.g. proportionate measures to secure public interest objectives).[36] As a result, the controller must seek an optimal balance between conflicting principles and values. In any case, EU law has set up a very complex multi-level system for assessing the processing of personal data, which places demands on the controller according to the complexity of the personal data it processes.

5. The Principle of Proportionality in the Data Protection Context

With regard to the principle of proportionality, which is an essential component of Article 52(1) of the EU Charter, at the outset it may be briefly mentioned that the search for the measure of things has its origins already in ancient culture. As Pavel Holländer[37] states, the origins of this concept can be found in 19th century German law, but it is only after the Second World War that the principle of proportionality has taken doctrinal form and spread horizontally and vertically to other legal orders and systems. Today, the principle of proportionality is applied as a measure of the limitation of fundamental rights in many, but not all, effective constitutional justice systems. For the sake of completeness, it should be noted that the U.S. constitutional development was and is moving in a different direction, with considerations of the proportionality of values (fundamental rights) stemming from its own historical and constitutional justice trends.[38] In general, the principle of proportionality is a complex abstract tool for measuring fundamental rights, which is not methodologically uniform and is the subject of academic disputes. It is generally true that the essence of the proportionality principle is preserved in case of compliance with the three-step test (appropriateness, necessity and proportionality in the narrower sense) and the principle of compliance of the legal order with the Constitution (constitutional values). However, the application of the proportionality principle does not follow an identical methodology, so there are substantial theoretical differences in this respect. Legal theory has developed complex conceptual constructions of the principle of proportionality, the key ones of which is the model of the prohibition

[36] Point 69 GDPR Preamble.

[37] Pavel Holländer, a former constitutional judge of the Constitutional Court of the Czech and Slovak Federal Republic and of Constitutional Court of the Czech Republic later on, introduced the principle of proportionality into Czech legal discourse.

[38] In the United States so-called balancing test is used as the way competing rights are measured.

of disproportionality (Peter Lerche), the principle of practical concordance (Konrad Hesse) and the interpretation of the principle of proportionality in terms of the command to optimise (Robert Alexy). Thus, it must be stated that there is no uniform methodology of the proportionality principle.[39] It is also important that, in terms of the application of the proportionality test, the decisive problem is often not the proportionality test itself, but the very identification of the rights that (actually) conflict or whose protection is at stake in the case in question.

In terms of content, the principle of proportionality is a designation for the balancing exercise used when two or more protected fundamental rights come into conflict. According to Pavel Ondřejek,[40] the principle of proportionality is based on the concept of the rule of law as an objective order of values in which fundamental rights play a central role. Along with the growing importance of fundamental rights in application practice, there is also a growing need to find an adequate methodology for dealing with conflicts between fundamental rights, or conflicts between a fundamental right and a constitutionally protected public interest. The advantage of this constitutional argumentation method is the maximum consideration of the context of the case, taking into account the facts of the case. The balancing of fundamental rights and public interests is normally conceived as a component of the principle of proportionality and is often described as an alternative method of applying the law alongside subsumption. When measuring, we look at the applied rules as legal principles, in the application of which we can consider the degree of their fulfilment in a particular case, not, as is the case with legal norms, the classification or non-classification of a factual situation under this legal norm.[41] In practice, the doctrine of proportionality is typically used by the highest judicial institutions, and it is also used by the ECHR and the CJEU; however, it is always used with a certain degree of variability, while maintaining the basic set-up as described above.

In data protection practice, the proportionality test is applied with a large degree of flexibility. Controllers, and sometimes also supervisory authorities, are not always able to use use the advanced and complex proportionality test under Article 52 (1) of the EU Charter; instead they use a simplified test, which they refer as the balancing test, although this term is not mentioned both in the GDPR and the CJEU case law. The so-called balancing test is problematic in

[39] HOLLÄNDER, P. *Příběhy právních pojmů*. Vydavatelství a nakladatelství Aleš Čeněk, s. r. o., Plzeň: 2017, pp. 198–231.

[40] Pavel Ondřejek is an associate professor at Charles University. He is the author of the monograph The Principle of Proportionality and its Role in the Interpretation of Fundamental Rights and Freedoms (Prague: Leges, 2012).

[41] ONDŘEJEK, P. Poměřování jako klíčový argument přezkumu ústavnosti v éře proporcionality a některé projevy jeho kritiky. Proportionality as a key argument of constitutional review in the era of proportionality and some of its criticisms. *Právník.* 2016, roč. 155, č. 4, pp. 349–368. Detail článku | Ústav státu a práva Akademie věd České republiky (cas.cz).