PWPM 2021, Vol. XIX
REVIEW OF INTERNATIONAL, EUROPEAN AND COMPARATIVE LAW
PROBLEMY WSPÓŁCZESNEGO PRAWA MIĘDZYNARODOWEGO, EUROPEJSKIEGO I PORÓWNAWCZEGO
ISSN 1730-4504

ARTICLES / ARTYKUŁY

DOI: 10.26106/0ptv-0g79

Regulating the digital environment: What can data protection law learn from environmental law?

Magdalena Słok-Wódkowska
Associate Professor (Dr. habil.) at the Faculty of Law, University of Warsaw
ORCID: 0000-0002-0108-2330, e-mail: m.slok@wpia.uw.edu.pl

Joanna Mazur
MA in Law, Ph.D. Student at the Faculty of Law, University of Warsaw
ORCID: 0000-0002-0417-5743, e-mail: j.mazur@delab.uw.edu.pl
The input of Joanna Mazur to the article was prepared as a part of the grant project 'Automated decision-making versus prohibition of discrimination in the European law' – funded by the National Science Centre, Poland: Project number 2018/29/N/HS5/00105

I. Introduction: The Metaphor of the 'Digital Environment'

The metaphor of the 'digital environment', which describes the results of the ongoing digital transformation, seems to be so commonly used that its literal connotation has become almost undetectable. It is present in both everyday language and in the documents which address the legal challenges arising from the growth of digital economy.[1] Its popularity might be the result of its accuracy: are we still capable of imagining our environment without any digital components? Is the digital environment a separate phenomenon, strictly linked to phenomena of Web 2.0, or rather, has the very environment in which we live become digital?

[1] The search for the term 'digital environment' had 669 results in the EUR-lex.europe.eu database (as for 20 May 2020). It should be however noted, that there are more expressions which confirm a conceptual link between the environment in its ecological meaning and the digital one, for example, 'digital footprint' (ecological footprint), data as a 'new oil', or the term 'text and data mining'.

The similarity between the natural environment and the developing digital one has not escaped the attention of scholars. The concept of digital environment was examined by D. D. Hirsch[2] and A. M. Froomkin,[3] both of whom wrote on the ways in which environmental law might inspire the regulation of data protection in the context of United States' (US) regulatory framework. It must be noted, however, that US regulations – concerning both environment and privacy – differ significantly from European Union (EU) law. Another study on this topic, written by M. J. Emanuel,[4] focuses on the comparison between the regulatory frameworks in the US and the EU and potential global regulations for data protection. As these differences are not merely procedural but also rooted in a different axiology, comparisons made in these analyses are not entirely relevant to EU law. It is also worth mentioning that the majority of these studies were conducted before the General Data Protection Regulation[5] (GDPR) entered into force.

Our approach is focused on the questions raised by the relationship between international law and the EU's legal order in terms of the development of legal measures common for environmental law and data protection law, as well as the principles standing behind these legal measures. Our work provides insight into this issue in the context of the European regulation of data protection. As we hope to show below, there are similarities between the legal instruments adopted in the area of data protection law (fundamental for the digital environment) and the legal instruments adopted in the area of environmental law (fundamental for the natural environment) in EU law. Therefore, it is worth scrutinising what kind of lessons may be learned from the development of environmental law in order to effectively develop regulations governing the digital environment.

The main hypothesis of the article is that the development of environmental law – which could provide an inspiration for the development of the regulatory dimension of the digital environment – indicates there is a need to fill the principles and rules of a general character with very specific normative content. In order to examine this hypothesis, we analyse the resemblance between the legal instruments

2 D. D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, Georgia Law Review 2006, vol. 41, no. 1.

3 A. M. Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, University of Illinois Law Review 2015, issue 5.

4 M. J. Emanuel, *Evaluation of US and EU Data Protection Policies Based on Principles Drawn from US Environmental Law* [in:] D. Svantesson, D. Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge 2017.

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 (General Data Protection Regulation) [2016] OJ L 119/1.

adopted in the area of European data protection law (GDPR) and European environmental law. In our analysis, we focus on the level of rules and sets of rules, and for the purpose of this analysis call the latter 'legal instruments'.[6]

Under the term 'legal instrument', for the purpose of this article, we understand a set of rules pertaining to the development of specific standards for a particular rule. Due to the highly abstract content of the principles, it is necessary to unravel the common understanding of their content. One of the ways of reaching this goal is to examine what kinds of legal instruments specify the principles' meaning and serve their execution. It is not a particular rule, but rather a set of rules, which create a precise and comprehensive regulatory framework concerning a certain issue. For example, impact assessment, as a legal instrument, consists of a set of rules regulating issues such as e.g. when to conduct an impact assessment, what should be considered when conducting impact assessment, who is allowed to participate in the process of conducting an impact assessment or who should have access to the results of one.

The structure of the article includes three main parts: firstly, we present the traditional division of legal norms into principles and rules, and our definition of the term 'legal instrument'. Consequently, the first part provides the overall framework for the analysis, focusing on 'legal instruments' as the foundation for ensuring a common understanding of abstract principles. Secondly, we analyse legal instruments of a specific character, which are implemented in the GDPR in order to execute the most abstract and general principle of data protection law: data minimisation. This principle stresses the need to perceive digital environment as a whole and to adopt precautionary and preventive approach to its regulation, which constitutes the similarity with the regulatory approach which is advised in terms of regulating natural environment. We focus on the legal instruments which implement this principle and are present both in data protection and environmental law, namely impact assessment (data protection impact assessment, DPIA), and legal instruments linked to the access to information (information obligations and right to access). Due to the novelty of DPIA and the new form that the access to information took in EU law, we conduct a doctrinal analysis of the GDPR's provisions. Thirdly, we highlight the similarity between the significance of data minimisation principle for data protection law and the precautionary principle in environmental law. We proceed with the analysis of the legal instruments in environmental law which implement the

[6] We shift the perspective presented by P. de Hert, who claims that 'principles can bridge differences in legal regimes and pave the way for common understanding of things (and eventually more common rules).' – P. de Hert, *Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules: Piercing the Veil of Stability Surrounding the Principles of Data Protection*, European Data Protection Law Review 2017, vol. 3, issue 1, p. 169.

precautionary principle, such as environmental impact assessments (EIA), the right to access information, the right to public participation and right of access to justice.[7] What constitutes the backbone of our analysis is the comparison of the legal instruments adopted in environmental law with the same types of legal instruments adopted in data protection law,[8] which provides inspiration for the discussion concerning the development of the legal instruments adopted in the area of European data protection law. The text ends with a number of conclusions.

II. Principles, Rules, and Legal Instruments: Overview of the Terminological Differences

The theoretical framework of this article is based on the well-established Dworkinian division of legal norms into two categories, namely principles and rules. The division forms a hierarchy based on the level of abstraction of the norms, the principles being more abstract than rules.[9] The principles serve as general guidelines of an axiological character. The principles envision the values inscribed in the regulation, but their abstract character makes it hard to actually define their content in terms of the obligations which they impose.[10] As principles can be difficult to define and therefore to execute, it is the rules which translate principles into more specific norms. Rules include more precise obligations and therefore provide the principles with specific content which can be reformulated into a yes or no question. One can either comply or not with a rule, while it is possible to comply with a principle only to a certain extent. For example, one either fulfils the obligation of including alternative analysis in an impact assessment or one does not (rule) but one can only follow the principle of data minimisation to a lesser or a greater extent (principle).

---

7 The assessment of the effectiveness of environmental law remains beyond the scope of our analysis. For the literature on this topic, see D. Petrić, *Environmental Justice in the European Union: A Critical Reassessment*, Croatian Yearbook of European Law and Policy 2019, vol. 15, issue 1, p. 215.

8 Our analysis of environmental law is limited to what is necessary for comparisons to data protection law, as we do not intend to analyse environmental principles, rules or instruments of environmental law *per se*.

9 See R. M. Dworkin, *The Model of Rules*, The University of Chicago Law Review 1967, vol. 35, issue 1, p. 23.

10 This might facilitate broad adoption of the principles in the international community, but it might also hamper the execution of the principles themselves: '...while it is difficult to agree on fixed and precise rules at the international level, it is far easier to come to a public understanding about indefinite principles that can progressively be given more concrete form' – N. de Sadeleer, *Environmental Principles: From Political Slogans to Legal Rules*, New York 2002, tr. S. Leubusher, p. 1.

For the purpose of this analysis, we claim that the rules often need very detailed specification, which leads to the formation of legal instruments. The rules as the 'practical formulation of the principles'[11] become comprehensive sets of provisions – legal instruments – which serve the implementation of the principles. In some areas of EU law legal principles are directly included in the fundamental legal acts constituting EU's legal order (as in the case of environmental law) and in others they are directly formulated in the legal acts fundamental for a particular area of regulation (as in the case of data protection law).

An example of the relationship between the principles, rules and legal instruments drawn from data protection law is the principle of lawful processing and the rules which include, for example, the provisions enumerating the grounds for the processing to be considered lawful: consent, required for the execution of the contract etc.[12] The rules which specify the requirements for consent form a specific legal instrument: consent understood in accordance with the GDPR's requirements.

Another example of the relationship between principles, rules, and legal instruments can be drawn from environmental law. Even in the EU law, there is a clear distinction between principles, which are of the very general nature, like the subsidiarity principle, and rules. There are no doubts, that (as confirmed in the *Artegodan* judgment) precautionary principle is also one of those general principles of EU environmental law,[13] which can be qualified as a Dworkinian principle.[14] The principle of preventive action and the precautionary principle – which are closely related[15] – may be translated to the rules by, among others, the implementation of an obligation to conduct an impact assessment. However, such an obligation is not enough to execute this obligation with sufficient precision. There is a need to implement specific provisions which regulate the details of when and by whom the impact assessment should be conducted, what it should include, who should be allowed access to its

---

11 P. Sands and others, *Principles of International Environmental Law*, Cambridge 2012, p. 189.

12 See European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxembourg 2014, pp. 62–67, 81–90.

13 Joined cases T-74/00, T-76/00, T-83/00, T-84/00, T-85/00, T-132/00, T-137/00 and T-141/00 *Artegodan GmbH and Others v Commission of the European Communities* ECLI:EU:T:2002:283.

14 See S. Kingston, V. Heyvaert, A. Čavoški, *European Environmental Law*, Cambridge 2017, p. 91; Y. Nakanishi (ed.), *Contemporary Issues in Environmental Law. The EU and Japan*, Tokyo 2016, p. 29.

15 Acknowledging that principle of prevention and precautionary principle are separate though closely related we use them both as principles that can be translated into rules and instruments of environmental and data protection law, see L. Krämer, *EU Environmental Law*, London 2012, p. 24.

results etc. The body of rules which refer to the general obligation of conducting impact assessment constitute a legal framework for such a legal instrument.

In short, the process which we describe is – in the first step – the implementation of rules which embody values adopted in the general principles. The second step is to specify the rules by adding additional requirements concerning their content. As a result, the development of legal instruments can be observed. As every legal subsystem needs principles as a frame or skeleton that needs to be filled with the muscles of rules, we intend to seek resemblance of principles of digital and natural environment and, as a result, the resemblance between rules in these areas.

As we argue on the basis of the formal-dogmatic analysis of the EU legal acts, it is possible to observe a certain dynamic within the complexity of the bodies of rules constituting legal instruments. Technological progress can enforce the process of more precise regulation of certain legal instruments, whereas more precise regulation of certain legal instruments can inspire the technological development of the solutions which incorporate values promoted by law. An example being the legal instruments developed during the evolution of environmental law, the function of which is to ensure the implementation of certain standards of environmental protection. This evolution in case of environmental law can be observed over a much longer period than is the case for data protection law. The difference in timing between the legal instruments adopted in the area of environmental law and in data protection law allows us to identify some trends in the evolution of environmental law which provide important insights into the legal instruments which have been adopted by data protection law. In order to be able to identify the common legal instruments for both of these areas of regulation, we start with a brief examination of data minimisation principle and the legal instruments in the GDPR which serve the purpose its execution, which state grounds for the comparison between the environmental law and data protection law presented in the subsequent section.

III. Background: Principles, Rules and Legal Instruments of Data Protection Law and the Role of the Data Minimisation Principle

The foundations for establishing the catalogues of the principles of data protection law in the international context have been shaped by the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[16] which were adopted

[16] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, source: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2.

in 1980,[17] and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) adopted by the Council of Europe in the following year.[18] In the case of European data protection law, the catalogue promoted by the OECD's guidelines has been to a great extent included in Art 5 of the GDPR. The principles enumerated therein provide an overall direction for the interpretation of rules and inform on the axiological background standing behind the rules implemented in the regulation.[19] Unlike the principles in international environmental law, these principles are in no way recognized as binding international law. Therefore, including them into EU law is the only way for them to become binding for the member states.

From this catalogue of principles, our focus on data minimisation is motivated by the fact that as the economic meaning of data grows, the shift to rules which stresses the necessity of limiting data collection itself seems to be necessary in order to effectively protect the users in the digital environment.[20] Data minimisation is also a principle which focuses on the requirements regarding the systems of data processing themselves (the digital environment in which processing takes place), not on the rights of data subjects. Thus, what it protects is the quality of technological solutions used for data processing. It, therefore, resembles solutions which are implemented in the area of environmental protection law as they are focused on protecting the environment itself.[21]

Data minimisation is a step in the direction of supporting data protection with additional requirements concerning personal data collection and processing. This is the data minimisation principle what links on the most general level of principles data protection law and environmental law. Firstly, it indicates the focus on preventive, precautionary measures as it is a guideline concerning the digital environment as a whole similarly to the principles of preventive action and precautionary principles in environmental law.[22] Secondly, the legal instruments implemented in the

---

17 Updated in 2013: OECD, *The OECD Privacy Framework*, 2013, source: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

18 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985) 108 ETS (Convention 108).

19 See L. A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford 2014, p. 145.

20 For the elaboration on the issue of implementing precautionary solutions in case of digital economy regulation see J. E. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism*, Oxford 2019, pp. 90–91, 102.

21 We would like to thank the anonymous reviewer for pointing out this issue.

22 For a detailed analysis of the precautionary principle in the context of data protection, see J. Mazur, *Automated Decision-Making and the Precautionary Principle in EU Law*, Baltic Journal of European Studies 2019, vol. 9 issue 4, p. 3.

GDPR as tools serving the realisation of the data minimisation principle, are closely linked to the legal instruments which have been developed in environmental law. As we argued above, the key aspect of the evolution of principles of data protection law lies within the dimension of the rules and, even more specifically, legal instruments adopted in order to ensure the holistic and precise approach to certain issues. In the next subsections we show in detail how the principle of data minimisation became a vital link between the data protection law and environmental law.

III.1 The Evolution of the Data Minimisation Principle

Even though the presence of the data minimisation principle can be traced back to EU Directive 95/46 ('Member States shall provide that personal data must be (...) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'),[23] in the GDPR both its description and its content has evolved. As all of the principles enumerated in Art 5(1) of the GDPR have been labelled, the minimality[24] principle has been called 'data minimisation'. Moreover, in the GDPR the formulation 'not excessive...' has been replaced with the phrase 'limited to what is necessary in relation to the purposes for which they are processed',[25] which seems to be more straightforward (or 'explicit'[26]) expression. The vestigial rules embodying the principle have been developed, and additional instruments serving the purpose of compliance with the data minimisation principle have been implemented to the regulation.

An example of such a notion is the implementation to Art 25 of the GDPR data protection by design and data protection by default.[27] We argue that data protection

[23] See Art 6, 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 [1995] OJ L 281/31. The CJEU referred to the principle in e.g. case C-342/12 *Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho* ECLI:EU:C:2013:355 or joined cases C-465/00, C-138/01 and C-139/01 *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk* ECLI:EU:C:2003:294, however its interpretation was limited to acknowledging the principle's existence.

[24] See L. A. Bygrave, *Data Privacy Law...*, *op. cit.*, pp. 151–152.

[25] See GDPR, Art 5.

[26] C. Kuner, *The European Commission's proposed data protection regulation: A Copernican revolution in European data protection law*, Privacy & Security Law Report 2012, vol. 6, issue 6, p. 5.

[27] For the analysis of the concepts see L. A Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, Oslo Law Review 2017 vol. 4, issue 2; D. W. Schartum, *Making privacy by design operative*, International Journal of Law and Information Technology 2016, vol. 24, issue 2; M. Veale, R. Binns, J. Ausloos, *When data pro-*

by design and by default are concepts which can be understood in two ways: firstly, as new general principles of data protection law and secondly, as rules which implement the principle of data minimisation. Lack of the relevant case law does not allow to unequivocally support one of the interpretations, therefore we present the arguments for both of them.

The interpretation of data protection by design and by default as principles is supported by the phrasing of some of the GDPR's provisions. In Art 47(2), which includes the enumeration of the conditions which should be met by binding corporate rules, the following catalogue of principles appears: 'The binding corporate rules (...) shall specify at least: the application of the general data protection principles, in particular (...) data minimisation, (...) data protection by design and by default'.[28] Such phrasing suggests the advancement of data protection by design and by default to general principles of the EU data protection law.

This interpretation of data protection by design and by default as principles is, however, not supported by the overall structure of the GDPR: data protection by design and by default are not included in the catalogue in Art 5, which shows a certain level of inconstancy on the part of the European legislator. Moreover, it must be noted that Art 25 links data protection by design and by default directly to the principle of data minimisation execution. As the provision deserves closer attention, we quote a substantial part of it:

> the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.[29]

Due to the content of this provision and exclusion of data protection by design and by default in the catalogue of data protection law principles included in Art 5, we suggest treating them as rules, which have not been sufficiently developed to form legal instruments yet.

The selection of the phrase 'measures (...) designed to implement data-protection principles' supports the above presented conceptualisation of the dynamics between principles, rules and legal instruments. Directly evoked in Art 25(1) principle of data minimisation is an ultimate, axiological goal, bundled with data protection

tection by design and data subject rights clash, International Data Privacy Law 2018, vol. 8 issue 2.

[28] See GDPR, Art 47(2).

[29] See GDPR, Art 25(1).

by design and by default rules. In yes or no, and much simplified, form, rules of data protection by design and by default could be put down to a question: did the controller, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles?[30]

Art 25 informs us who is obliged to implement organisational and technical measures, when, under what conditions, what is the goal of such an activity etc. However, due to the limited development of rules constituting the content of data protection by design and by default, they do not seem to create a sufficiently precise set of rules to be perceived as legal instruments. In order to better understand this issue, it is necessary to further scrutinise the meaning of the term 'technical and organisation measures' used in Art 25.

III.2 In Search of 'Technical and Organisational Measures' in the GDPR

The definitions of data protection by design and by default provided by the GDPR refer to 'technical and organisational measures', specifying solely pseudonymisation as an example of such. Recital 78 of the GDPR additionally refers to transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, and enabling the controller to create and improve security features.[31] These examples may be perceived as having a more organisational character – but they are missing the legal content of specific legal norms which should be implemented. We argue that the implementation of data protection by design and by default to the GDPR seems to lack the precise indicators which would allow assessing the compliance with the standards set by them. Due to this reason, it also blurs the content of data minimisation principle, as data protection by design and by default rules are meant to implement this and other data protection principles. There are two possible solutions to this conundrum. The first – already criticised in the literature[32] – is to rely on 'technical measures' as

30 See GDPR, Art 25(2), concerning data protection by default, seem to be to a certain extent redundant, as it includes a description of the necessary measures which should be implemented for 'ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'. Such obligation may be perceived as part of the data minimization principle realization.

31 See GDPR, recital 78.

32 For such a critique, see B.-J. Koops, R. Leenes, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law*, International Review of Law, Computers and Technology, 2014, vol. 28, issue 2; M. Pocs, *Will the European Commission be able to standardise legal technology design without a legal method?*, Computer Law & Security Review 2012, vol. 28.

means to execute the legal rules. The second is to examine whether there are 'organisational measures' implemented in the GDPR which could be perceived as legal instruments which might ensure the execution of data protection by design and by default, even though they are not explicitly related to these rules. We briefly examine both of the indicated options.

Considering the approach based on 'technical measures' to support the regulation of privacy, as B.-J. Koops and R. Leenes[33] indicate, there is no clarity in terms of the level on which the data protection by design and by default tools should be implemented: are these system level requirements? Or for example language requirements? There is no common agreement on the technical meaning of these concepts. These reasons show that the assumption that referring to 'technical measures' may clarify the legal meaning of rules such as data protection by design and by default is, in the best-case scenario, naïve. It also seems to leave the regulatory provisions helpless in the face of technological challenges, while it is possible to claim that regulation can inspire the pursuit of technological solutions.

In terms of the second possibility – considering 'organisational measures' implemented to the GDPR as signs of data protection by design and by default execution – it must be stressed that this interpretation must be supported by the teleological interpretation of the GDPR. There are no indicators which explicitly link legal instruments adopted in the GDPR with data protection by design and by default. There is, however, space to interpret legal instruments adopted in the GDPR as the means to achieve selected aims enumerated in relation to the data protection by design and by default (and therefore, data minimisation principle) in recital 78 of the GDPR. As the examples we may indicate the following legal instruments:

(1) Goal 'transparency with regard to the functions and processing of personal data': DPIA, certification, codes of conduct;
(2) Goal 'enabling the data subject to monitor the data processing': information obligations, right to access, information on data breach;
(3) Goal 'enabling the controller to create and improve security features': no relevant legal instruments identified.[34]

In terms of the execution of transparency with regard to the functions and processing of personal data, it is necessary to indicate the auditing mechanisms[35]

[33] B.-J. Koops, R. Leenes, *op. cit.*, p. 164.

[34] Despite the best efforts of its authors, none of legal instruments included in the GDPR seem to be mainly focused on the aim of enabling the controller to create and improve security features.

[35] We use this catalogue as formulated by B. W. Goodman, *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection*,

included in the GDPR: DPIA, certification mechanisms and codes of conduct as organisational legal instruments to ensure compliance with the rules of data protection by design and by default. These measures seem to constitute legal instruments which in theory could support the goals enlisted as objectives of data protection by design and by default rules: their role is to increase the transparency and facilitate communication concerning specification of some of the GDPR's provisions. Organisational instruments which may support enabling the data subject to monitor the data processing include information obligations, right to access and information on data breaches. However, the details of the adoption of these organisational legal instruments in the GDPR, if interpreted in light of data protection by design and by default rules – and therefore, as legal instruments serving the purpose of the data minimisation principle, leaves considerable room for improvement.

III.3 Room for Improvement: Inefficiencies of the Adopted Instruments

Two of the three auditing instruments implemented in the GDPR's provisions, namely certification mechanisms and codes of conduct, lack an obligatory character. It constitutes a drawback of the solutions adopted in the GDPR. Only DPIA has an obligatory character in selected cases, the range of which will to a certain extent depend on decisions of the supervisory authorities. The supervisory authorities shall establish and make public a list of the kind of processing operations which are subject to the requirement of conducting a DPIA.[36] The overall indicators of what type of processing should be subjected to a DPIA includes the possibility that a type of processing – in particular using new technologies – is likely to result in a high risk to the rights and freedoms of natural persons.[37] When assessing the risk, the nature, scope, context and purposes of the processing should be taken into account. In detail, Art 35(3) indicates that a DPIA shall be required in the case of (1) a systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing and on which decisions are based that produce legal effects or similarly significant effects; (2) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; (3) a systematic monitoring of a publicly accessible area on a large scale.

29th Conference on Neural Information Processing Systems, Barcelona, 2016, source: http://www.mlandthelaw.org/papers/goodman1.pdf.

36 See GDPR, Art 35(4).

37 For the analysis of this issue see N. van Dijk, R. Gellert, K. Rommetveit, *A risk to a right? Beyond data protection risk assessments*, Computer Law and Security Review 2016, vol. 32, issue 2, and – in the context of similarity with environmental law – R. Gellert, *Understanding the notion of risk in the General Data Protection Regulation*, Computer Law and Security Review 2018, vol. 34, issue 2.

The scope of the types of processing which should lead to conducting an obligatory DPIA allows the claim that this instrument could become an important tool of execution of data protection by design and by default rules.[38] However, the transparency of the DPIA should be the subject of a careful revision: if a DPIA was to function as an instrument to implemented data protection by design and by default rules transparency, it should follow the above-mentioned guidelines on the meaning of these rules, for example, enabling transparency with regard to the functions and processing of personal data. The final shape of the GDPR's provisions concerning the DPIA, limits the possibility of data subjects or their representatives' participation in this procedure. According to Art 35(9) the controller – where appropriate – shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.[39] Moreover, the broader public will not be informed of the outcomes of a DPIA, which further limits the possible scope of its influence on the level of transparency regarding data processing. DPIA remains a tool which can be used between data controllers and administration,[40] not subject to the direct control of the users.[41]

Similar objections should be raised in relation to the instruments which address the guideline to enable the data subject to monitor the data processing as a part of the data protection by design and by default rules. The debate concerning the 'right to explanation'[42] based on the right to access, and its dubious character in the GDPR

[38] For such an approach, see, L. Edwards, M. Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, IEEE Security and Privacy, 2018, vol. 16, issue 3, pp. 46, 50–51; B. Casey, A. Farhangi, R. Vogl, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, Berkeley Technology Law Journal 2019, vol. 34 pp. 145, 173–174.

[39] See GDPR, Art 35(9).

[40] In terms of consultations defined in GDPR, Art 36(1).

[41] This interpretation of the GDPR has been confirmed by Article 29 Data Protection Working Party document: 'Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA' – Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 17/EN' (WP 248 rev.01, 4 October 2017), p. 18.

[42] For detailed analysis of the adopted provisions 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*, International Data Privacy Law 2017, vol. 7, issue 2; A. D. Selbst, J. Powles, *Meaningful information and the right to explanation*, International Data Privacy Law 2017, vol. 7, issue 4; G. Malgieri, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, International Data Privacy Law 2017, vol. 7, issue 4; M. Brkan, *Do algorithms rule the world? Algorithmic decision-making and data protec-*

shows the inefficiencies of the adopted provisions. As it has been subjected to thorough analysis, we only briefly indicate reasons for looking for additional solutions concerning the execution of an individual's rights in a digital environment.

Technically, the right to access should, among others, grant the data subject meaningful information on the logic involved in the automated decision-making process. However, the information on the logic involved should be offered when the decision is based solely on automated decision-making tools – which raises doubts concerning the meaning of the term 'solely'. Moreover, the decision has to produce the legal effects or a similarly significant result for the individual, which is yet another limitation of the possible scope of the situations in which such information will be presented to data subjects. A lack of clarity concerning what terms used in the provision, for example, 'meaningful information', or 'decision' mean, constitutes further obstacles for perceiving the 'right to explanation' as a tool ensuring the transparency of data processing. Moreover, the provisions adopted in the GDPR seem to be focused on an individual and her rights. These means that group privacy[43] is not sufficiently addressed as such by the GDPR. The provisions concerning information obligation and information on data breaches share this characteristic with the 'right to explanation': we may know who is getting our consent for the processing or receive communication concerning the data breach, but we are lacking the bigger picture.

While we do not claim that the proposed catalogue of the legal instruments indirectly implementing data protection by design and by default rules is exhaustive, it does provide sufficient grounds for conducting a comparison between the form these legal instruments take in the GDPR and the EU environmental law. We argue that it not only informs us of the inefficiencies of the adopted provisions but also shows the source of potential inspirations for improvement. The choice of impact assessment as an instrument relevant for data protection law has a historic background of the developments in the area of environmental law. This has been noted in the literature referring to the GDPR, for example, 'the concept of a PIA is derived from instruments in other policy areas like environmental law'[44] and 'amongst the novelties here are the introduction of mandatory data protection impact assessments (following the example of environmental law)'.[45] Moreover, the broadly

tion in the framework of the GDPR and beyond, International Journal of Law and Information Technology 2019, vol. 27, issue 2.

43 For more on this category see, for example, L. Taylor, L. Floridi, B. van der Sloot (eds), *Group Privacy. New Challenges of Data Technologies*, Cham 2017.

44 R. Binns, *Data protection impact assessments: a meta-regulatory approach*, International Data Privacy Law 2017, vol. 7, issue 1, p. 23.

45 P. de Hert, *op. cit.*, p. 174

discussed 'right to explanation' could be perceived as an individually-focused right to access information, also a vital element of environmental law principles. Even though the effectiveness of instruments adopted in the area of environmental law may raise doubts, it can be perceived as a source of – if not an inspiration – then of experiences, which could provide valuable insights for the improvements of data protection law. In the following section, we examine this issue in more detail.

IV. Results: The Development of Environmental Law and Lessons for the Digital Environment (Impact Assessments, Access to Information and Access to Justice)

The current form of environmental provisions in the EU Treaties as well as in secondary legislation has been shaped throughout several decades since the 1980s, evolving from the very general to something much more specific. This provides a circa 15 years longer perspective than the development of European data protection law. However, contrary to data protection law, the principles of environmental law are not only already subject of definition in the EU, but also backed by its counterpart in international environmental law which results with additional experiences concerning the attempts to develop legal instruments ensuring the implementation of the environmental law principles. Our analysis is focused on the comparison of the solutions implemented to the EU environmental and data protection law, however, in certain cases it is necessary to refer to its international roots, for example, considering the impact of the adoption of the Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention)[46] on the content of the EU directives. Although the Aarhus Convention is an international agreement concluded within United Nation Economic Commission for Europe, is open for accession for regional integration organization. Therefore, as the EU is a party to the Aarhus Convention, it is obliged to implement it both on the level of the EU and of the member states.

It must be stressed that this core section of the paper is based on the approach according to which the division on principles, rules and legal instruments that we presented above, is relevant for environmental law. The role of rules and legal instruments is crucial for the specification of the principles' normative content, which themselves not always clearly defined. The above-mentioned evolution of environmental regulation from more general to much more specific shows the importance

[46] Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (adopted 25 June 1998, entered into force 30 October 2001) 2161 UNTS 447 (Aarhus Convention).

of the legal instruments' development for the execution of the principles. Such a notion is clearly discernible in EU environmental law, which introduces legal instruments in order to specify the meaning of the general principles and ensure the existence of measures which support their enforcement. Our analysis presents respectively environmental impact assessments and legal instruments implemented as the results of the adoption of the Aarhus Convention, namely access to information, the right to public participation and access to justice, as the legal instruments which serve the realisation of the precautionary principle.

The reason to focus on the precautionary principle is that it is centred on preventing activities which may result in considerable harm to the environment or public health.[47] As such, it resembles the data minimisation principle, which is also focused on damage control by limitation of data collection and processing in the first place. The precautionary principle, created in the 1980s, gained its popularity in international instruments since the Rio Conference in 1992,[48] where it was acknowledged as principle 15 of the Rio Declaration on Environment and Development.[49] It has its basis in the Treaty establishing the European Community,[50] also since 1992, with the amendment of Art 130. Currently it serves as one of the basic principles of European environmental law enumerated in Art 191(2) of the Treaty on the Functioning of the European Union[51] but also more generally a principle of EU law, serving as a tool and a basis for acting and taking precautionary and preventive measures even in a situation when the reality and seriousness of risks not

47 Which was confirmed in numerous judgments of international tribunals such as International Tribunal for the Law of the Sea and International Court of Justice. See: *Southern Bluefin Tuna (New Zealand v. Japan; Australia v. Japan),* Provisional Measures, Order of 27 August 1999, ITLOS Reports 1999, p. 280, par. 79–80; *MOX Plant (Ireland v. United Kingdom),* Provisional Measures, Order of 3December 2001, ITLOS Reports 2001, p. 95, par. 71; *Land Reclamation in and around the Straits of Johor (Malaysia v. Singapore),* Provisional Measures, Order of 8 October 2003, ITLOS Reports 2003, p. 10, par. 71, 92; *Request for an Examination of the Situation in Accordance with Paragraph 63 of the Court's Judgment of 20 December 1974 in the Nuclear Tests (New Zealand v France)* Case, Dissenting Opinions of Judge Palmer and Judge Weeramantry, ICJ Reports 1995, p. 411–412 and 342–344.

48 N. de Sadeleer, *op. cit.*, p. 98.

49 'In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation' – Rio Declaration on Environment and Development, source: http://www.unesco.org/education/pdf/RIO_E.PDF.

50 Treaty establishing the European Community (Consolidated version 2002) [2002] OJ C 325/33.

51 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.

yet become fully apparent.[52] However, the precautionary principle has very vague content; therefore, to be fully implemented, it needs rules and the legal instruments formed by them.

IV.1 Evolution of Environmental Impact Assessment as the Legal Instrument Which Implements Precautionary Principle

One such instrument serving as a clarification of how the precautionary principle can be exercised is the EIA and the procedural requirements related to it. The concept of EIA has been developed simultaneously to the development of the precautionary principle itself: an essential part of the precautionary principle is the assessment of risks,[53] therefore a properly conducted impact assessment is an instrument which allows the fulfilling of this requirement. The first Directive on the assessment of the effects of certain public and private projects on the environment was issued in 1985,[54] as the first international (although in this case only EU-wide) instrument on EIAs.

Over time, not only did EU law on environmental impact assessment expand, but impact assessment also became one of the basic rules that led to the development of various legal instruments of international environmental law. As was confirmed by the International Court of Justice in the ground-breaking judgment *Pulp Mill*,[55] there is an obligation in general customary international law to pursue an EIA in the case of an undertaking that is likely to cause harm to the environment, even though there are no procedural guidelines and specific requirements enshrined in such a general obligation. Therefore, although a given state has to pursue an EIA, there is no clarity in international law concerning specific requirements, such as, for example, is it necessary to conduct public consultations, perform the comparison of alternatives or ensure access to information for other parties or stakeholders. There are not only various forms of environmental impact assessment (e.g. strategic or conducted by an investor) but also various models.[56]

---

52 Joined cases T-74/00, T-76/00, T-83/00, T-84/00, T-85/00, T-132/00, T-137/00 and T-141/00..., *op. cit*., para 185.

53 L. Krämer, *EU Environmental...*, *op. cit.*, p. 23.

54 Council Directive 85/337/EEC of 27 June 1985 on the assessment of the effects of certain public and private projects on the environment (Directive 85/337/EEC) [1985] OJ L 175/40.

55 *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, ICJ Rep 2010, 14, 82–84 (paras 203–206).

56 R. V. Burtlett, P. A. Kurian, *The Theory of Environmental Impact Assessment: Implicit models of policy making*, Policy & Politics 1999, vol. 27, issue 4; More on other international conventions including EIA see also: A. Epiney, *Environmental Impact Assessment*, Max Planck Encyclopedia of Public International Law (online), OUP.

Diversification of the requirements and procedural obligations concerning EIA leads to the possibility to achieve various goals by following the general obligation to perform EIA. Some of EIA procedures are purely pursued for a so-called window dressing or symbolic reasons. While other environmental assessment schemes are designed to provide information or help to avoid financial risks. Some forms of clarifying such requirements have been included in various international instruments, e.g. in the Espoo Convention on Environmental Impact Assessment in a Transboundary Context.[57] Although it is a general instrument concerned exclusively with impact assessment, procedural norms relate only to the setting of framework for transboundary cooperation, omitting all aspects of how exactly an EIA should be conducted. There are more procedural requirements in some other international conventions, but they have a more limited scope.[58]

As the international instruments are not usually suitable for achieving the requisite consensus to establish a clearly defined and detailed procedure for environmental impact assessment, they usually solely include more general principles.[59] EU law, on the other hand, enables establishing such detailed requirements. The procedure chosen for EIA by the European legislators can be perceived as detailed and designed to provide information for better-informed choices.[60] The first directive concerning EIA was fairly rough, even though an essential part of it were procedural requirements concerning the assessment such as mandatory public consultation and transparency.[61] Both of those features were developed over time, with the major change in 2003,[62] when the Directive was amended in order to adjust it to the requirements of the Aarhus Convention, on which we elaborate below.

Nowadays, it is the Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment, as amended by a Directive

---

57 Convention on Environmental Impact Assessment in a Transboundary Context (adopted 25 February 1991, entered into force 10 September 1997) 1989 UNTS 309.

58 E.g. the United Nations Convention on the Law of the Sea requires the publishing of reports, see Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 3 Art 205; and The Convention on Biological Diversity calls for public participation while conducting an EIA, see Convention on Biological Diversity (adopted 5 June 1992, entered into force 29 December 1993) 1760 UNTS 79 Art 14.

59 N. Craik, *The International Law of Environmental Impact Assessment. Process, Substance and Integration*, Cambridge 2008, p. 163.

60 S. Kingston, V. Heyvaert, A. Čavoški, *op. cit*., p. 381.

61 Directive 85/337/EEC, Art 6.

62 Directive 2003/35/EC of the European Parliament and of the Council of 26 May 2003 providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment and amending with regard to public participation and access to justice Council Directives 85/337/EEC and 96/61/EC [2003] OJ L 156/17.

2014/52/EU[63] that provides for detailed requirements to be implemented by the EU member states. It regulates in detail which undertakings and investments should undergo an EIA, dividing them into two basic categories of projects. It also states details concerning how and by whom an EIA should be conducted. Requirements concerning the scope of the EIA and a report are harmonised. The Directive also requires that the local authorities are at least consulted before taking a decision based on an EIA. Moreover, the EU not only retained requirements concerning public participation and access to information during the process but created regulations on how it should be performed. Equally detailed is a directive concerning a strategic environmental assessment – Directive 2001/42/EC on the assessment of the effects of certain plans and programmes on the environment.[64] This brief catalogue of precisely formulated requirements shows that EIA evolved from fairly unspecific rules into a comprehensively regulated legal instrument. The question which should be stated is whether this evolution of EIA may provide any inspiration for further development of DPIA.

IV.2 The EIA in European Law Compared to the DPIA

The following subsections analyse the provisions of the Directive 2011/92/EU which provide important examples for possible improvements to the DPIA. We organise our analysis according to selected model elements of EIA.[65] Thus, our analysis is focused on the selected differences between EIA and DPIA regulations concerning the stages of (1) screening, (2) scope and the contents of EIA reports, (3) notification and consultation, and (4) public participation and (5) final decision, which could provide inspiration for the further development of the DPIA.

---

[63] Directive 2011/92/EU of the European Parliament and the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment (codification) OJ 2012 L 26/1, as amended by a Directive 2014/52/EU of the European Parliament and the Council of 16 April 2014 (Directive 2011/92/EU) [2014] OJ L 124/1.

[64] Directive 2001/42/EC on the assessment of the effects of certain plans and programmes on the environment [2001] OJ L 197/30 (SEA Directive).

[65] Model elements usually named in the literature are: screening, scope and the contents of EIA reports, notification and consultation, public participation, final decision, post-project monitoring, strategic environmental assessment, implementation – e.g. N. Craik, *op. cit*., pp. 133–161; R. K. Morgan, *Environmental impact assessment: the state of the art*, Impact Assessment and Project Appraisal 2012, vol. 30, issue 1, p. 9. Due to lack of comparable elements in terms of prost-project monitoring, strategic environmental assessment and implementation we decided to exclude these stages from our analysis. For other examples of enumeration of EIA elements see V. P. Nanda, G. (Rock) Pring, *International Environmental Law and Policy for the 21st Century*, Leiden 2013, pp. 186–188.

Concerning the screening stage, since the first adoption of the EIA Directive in 1985 it contained two types of projects subject to an EIA: the annex with a list harmonised on the community level, which enumerated projects subjected to obligatory EIA and the list of the projects which could be subject to EIA on the basis of the member states decision. In the GDPR there are three selected types of processing subject to a DPIA on the basis of the GDPR provisions.[66] Moreover, the supervisory authorities in the member states shall establish, make public and communicate to the European Data Protection Board (EDPB) a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.[67] What is missing in the GDPR, is the common European list of the types of processing which should be subject to the DPIA. Even though the EDPB may play a role in the process of achieving common standards between the member states, it does not have the power to pursue its agenda in this regard. Therefore, the differences between the member states concerning the lists of processing operations which are subject to the DPIA cause differences in the standards of protection. The solution adopted in the case of the EIA Directive provides an inspiration for the further development of the organisational measures concerning the DPIA.

In regard to the scope and the contents of DPIA and EIA reports, there seems to one crucial element missing in the DPIA, namely alternatives analysis.[68] While the developer of the project which has an impact on the natural environment is obliged to consider the alternatives and provide reasons for not choosing them, the data controllers seem to function in a 'there is no alternative' paradigm. This should raise questions concerning the compliance of such an approach with the content of the data minimisation principle: can the DPIA answer the question of whether the collection and processing of data is 'limited to what is necessary in relation to the purposes for which they are processed',[69] while not comparing the planned processing with the possible alternatives? It must be stressed, that EIA itself went through a transformation in regard to the approach towards the alternative analysis. The 1985 version of the Directive annex III included the provision concerning the scope of the EIA: 'where appropriate, an outline of the main alternatives studied by the developer and an indication of the main reasons for his choice, taking into account

66 See above and GDPR, Art 35(3).

67 See GDPR, Art 35(4).

68 Art 5(1) includes the following element: 'a description of the reasonable alternatives studied by the developer, which are relevant to the project and its specific characteristics, and an indication of the main reasons for the option chosen, taking into account the effects of the project on the environment' – Directive 2011/92/EU, Art 5(1).

69 See GDPR, Art 5.

the environmental effects'.[70] With time, the phrase 'where appropriate' disappeared, as it appears that the alternative analysis is always appropriate, and the alternative analysis became an immanent element of the EIA. Such an evolution is a source of inspiration for the further development of the DPIA.

The stage of notification and consultation is at the core of the differences between the approach adopted towards the EIA and the DPIA in European law. The 1985 version of the Directive already contained provisions which addressed this issue:

> …the 1985 EC Directive on Environmental Impact Assessment [required] that the public have the opportunity to express an opinion before development consent is granted, that such views be taken into consideration by the government decision-makers, and that the public be provided with information on the decision outcome.[71]

The guarantees were included in Art 6(2), which obliged member states to ensure that any request for development consent and any information gathered pursuant to Art 5 of the Directive are made available to the public. The evolution of the Directive led to the adoption of a broad and specific catalogue of types of information which should be provided to public concerned.[72] These solutions are absent in the case of the DPIA. There are no obligations for the data controller to publish documents which are the results of a DPIA or the consultations with supervisory authority implemented by the Art 36(1) of the GDPR which proves DPIA is a legal instrument of an internal character. The broader public will not be informed of the outcomes of the DPIA, which may limit the possible scope of its influence on the level of transparency regarding data processing.

The only provision which mentions involving data subjects or their representatives in the context of DPIA is not only unclear in terms of its scope ('Where appropriate…'), but also limited by the exceptions included in the content of the provision ('without prejudice to the protection of commercial or public interests or the security of processing operations').[73] This proves that the DPIA remains a legal instrument which is not subject of any kind of obligatory direct control from the perspective of the public concerned. Whereas, since the adoption of the 1985 EIA Directive, the public concerned has been given the opportunity to express an opinion before the project is initiated.[74] Moreover, the Aarhus Convention had an impact on the direction of environmental regulation in the EU, inspiring a more

[70] Directive 85/337/EEC, Annex III: Information Referred to in Article 5(1).
[71] V. P. Nanda, G. Pring, *op. cit.*, 54.
[72] Currently included in the Art 6(2) and (3) of Directive 2011/92/EU.
[73] See GDPR, Art 35(9).
[74] Directive 85/337/EEC, Art 6(2).

transparent and participatory character of the adopted solutions.[75] These standards may inspire the data protection law in as they institutionalise the role played by the NGOs, associations and groups of people. As we discuss further in the article, such an approach could become an inspiration for data protection law, as it is also dealing with, on the one hand, highly specialised issues, and on the other hand – issues which have an impact on whole groups of people. Therefore, the very limited presence of NGOs and associations in the GDPR[76] should be expanded.

The stage of the final decision is the clearest example of the differences between EIA and DPIA. In the GDPR it depends entirely on the controller what will be the result of conducting DPIA. With the exception of the consultation with supervisory authority defined in Art 36(1), which should take place prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, there are no other results of DPIA foreseen by the GDPR. It supports the claim that DPIA remains an instrument of an internal character. In the case of EIA, there is no possibility of the competent authority not to get involved in the process leading to the final decision (development consent) of EIA. The decision to grant development consent, according to the Art 8a of the Directive 2011/92/EU, is made by the competent authority, after conducting impact assessment and after consulting public concerned. The competences of the state concerning EIA and the natural environment are by far more extensive than in case of DPIA and the digital environment. Similarly, the competences of the public concerned.

IV.3 The Access to Environmental Matters, Public Participation and Access to Justice in the EU Environmental Law as Legal Instruments Serving Transparency

It must be noted that what in the case of data protection law seems to be limited to the right to access information, environmental law has a broader scope in the case of the legal instruments developed in the EU. It not only includes access to information, but also a right to public participation and a right of access to justice, which is the results of the obligations for the EU and its member states arising from

[75] See N. de Sadeleer, *EU Environmental Law and the Internal Market*, Oxford 2014, p. 184. However, it should be also noted that the Aarhus Convention was inspired by the directives adopted by, then, EC: P. Oliver, *Access to Information and to Justice in EU Environmental Law: The Aarhus Convention*, Fordham International Law Journal 2013, vol. 36, p. 1425.

[76] An example being Art 80 of the GDPR which concerns representation of data subjects, discussed in the section 'Access to Justice as an Instrument to Support Accountability': see GDPR, Art 80.

the Aarhus Convention. The Aarhus Convention triggered some internal EU law implementing the Aarhus Convention both on the European institutions level[77] as well as directives concerning the decision-making process, public participation and access to justice in environmental matters within EU member states.[78] It also influenced some other EU legal acts, such as the above-mentioned procedures of EIA within the EU.

The Aarhus Convention seems like a realisation of a general rule of public participation in environmental matters. Although its roots can be traced back to the Rio Declaration and its principle 10,[79] it is the Aarhus Convention that in fact provides for a clear and relatively precise legal framework for this rule, as it is the most important international instrument concerning procedural rights in environmental matters.[80] Moreover, due to its cross-cutting impact on the transparency standards in environmental law, it should be perceived as a regulatory framework which defines a number of legal instruments serving the purposes enshrined in the precautionary principle.

The Aarhus Convention contains three equally important and interconnected pillars. The first of them is access to environmental matters. This can include both information on the state of the environment as well as policies and measures taken by, for example, states or other entities. It constitutes clear, sufficiently defined procedural requirements such as a period during which the information requested needs to be provided. It also defines exact reasons for which such information can be declined. Additionally, it requires that these reasons should be interpreted in a restrictive way. Information was divided into two kinds – one accessed only on request and the other that should be publicly available through 'public telecommunication networks' (Art 5(3)). Such a division, on the one hand, gives full access

---

77 Regulation (EC) No 1367/2006 of the European Parliament and of the Council on the application of the provisions of the Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters to Community institutions and bodies [2006] OJ L 264/13.

78 Mainly: Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC [2003] *OJ L 41/26;* Directive 2003/35/EC of the European Parliament and of the Council of 26 May 2003 providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment and amending with regard to public participation and access to justice [2003] OJ L 156/17.

79 See Rio Declaration, *op. cit*., principle 10.

80 N. de Sadeleer, *op. cit.*, p. 280; J. Jendrośka, *Introduction Procedural Environmental Rights in Theory and Practice* [in:] J. Jendrośka, M. Bar (eds) *Procedural Environmental Rights: Principle X in Theory and Practice*, Cambridge 2018.

to information, and on the other protects some sensitive data by making it available through harder to get on request.

The second pillar is public participation in the decision-making process in environmental matters. The Convention requires that the public should be informed through public notices or individually about certain activities, draft legal acts, plans, programmes and policies (enumerated in Arts 6, 7 and 8) of a state. It at least guarantees that interested entities are able to consult them. This pillar of the Aarhus Convention is even more detailed in the EU law, where it was implemented not only in the above-mentioned legislation directly aimed to implement the Aarhus Convention but also in more general acts.[81] On the EU level Regulation 1367/2006 sets an exact timeframe for obtaining comments as well as the requirement of identification of the affected public.

The third pillar of the Aarhus Convention is the most difficult to implement, but is of great importance if one takes into account that the sole right to information and public participation would be a dead letter if beneficiaries were deprived of the right to challenge decisions taken by the administration.[82] A key issue here is that the access to justice has been given not only to those whose rights have been allegedly infringed but also to non-governmental organisations (NGOs) acting as advocates for the environment generally. It proves how important role NGOs play in procedural rights related to the environment.

All the above-mentioned legal instruments play a crucial role in a process of translating general principles, established for decades in environmental law, into more detailed and precise rules and legal instruments. They create procedural rights and obligations that are in fact legal instruments for the implementation of, among others, very general and vague by itself, the precautionary principle. They have a horizontal effect and constitute an obligatory part of not only environmental law and policy-making, but also play an important role outside a field of environmental protection, for example, during the investment process. Such a broad impact on the whole area of regulation may provide important insight into how to improve provisions regulating similar legal instruments in the area of data protection, which we discuss separately; firstly, for the right to environmental information and public participation, and secondly, for the right to access to justice in the subsequent sections.

---

81 L. Krämer, *The EU and Public Participation in Environmental Decision-Making* [in:] J. Jendrośka, M. Bar (eds), *op. cit*., p. 132.

82 N. de Sadeleer *op. cit.*, p. 287.

IV.4 Evolution of the Right to Environmental Information and Right to Public Participation in European Law Compared to the Information Obligation in the GDPR

Environmental law can be perceived as a unique laboratory for the development of a broader right to access information. The Aarhus Convention has had an especial impact on the direction of environmental information regulation, inspiring a more transparent and participatory character of the adopted solutions.[83] A similarly pro-active approach has been presented by the European Court of Human Rights case law, which, for example, enabled linking the right to access information on the environment with the right to private and family life.[84] What seems to be a crucial characteristic of the right to access environmental information is the fact that it is not only perceived as a right by itself, but also serves as a measure to execute other rights. The most important example, which is stressed in the European legal acts, is the necessity to be properly informed in order to participate actively in the decision-making concerning environmental issues.

This is an important difference between the approach adopted in environmental law and data protection law. The environmental information serves – ideally – the bigger purpose of active, informed and collective participation in decision-making,[85] whereas the information obligations in the area of data protection do not serve such a purpose. They do not lead to the involvement of data subject in shaping of the data collecting and processing ecosystem or to voice one's opinion on these matters. Even the right to access, allowing the data subject to receive information on the processing, which has been perceived as a tool expanding the data subject's possibilities concerning the verification of the lawfulness of processing activities, is not different in this regard.[86] It can serve the purpose of the subject executing his or her rights by means of the data – it does not, however, provide access to information

[83] N. de Sadeleer, *op. cit.*, p. 184; V. P. Nanda, G. Pring, *op. cit*., p. 50.

[84] Throughout this motion, the ECHR enabled to oblige states to actively share information about the environment, due to the potential impact on family life of the citizens. For detailed analysis: N. de Sadeleer, *op. cit.*, pp. 114–22.

[85] 'In order to ensure the effective participation of the public concerned in the decision-making procedures, the public shall be informed…' – Directive 2011/92/EU, Art 6(2); 'The right is closely connected to participation rights in environmental impact assessment procedures and decision-making processes and with the development of procedural rights in human rights law' – P. Sands and others, *op. cit.*, p. 648.

[86] 'The right to access shall increase fairness and transparency of data processing as it permits data subjects to verify the lawfulness of processing activities performed on their personal data and will, thus, ultimately help to effectively enforce the data subjects' rights under the GDPR' – P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham 2017, p. 150.

which could support the collective involvement of groups, associations, or NGOs in data protection governance.

The individualistic perspective on the data protection related issues results with the exclusion of the broader context from the scope of information which should be provided to the data subject. In the case of the environmental information, what should be stressed is the fact that information in question refers to the environment in a more general, holistic perspective.[87] Moreover, the access to information in the case of environmental law is not bound with an interest having to be stated.[88] These are main characteristics which distinguish the approach towards information obligation in the digital environment and the ones which are subject to regulation concerning an environment. When pursuing this comparison, one could claim that data – as is often underlined in the public discourse concerning the digital economy – is a raw material to be used. The question which most of the information obligations in the GDPR answer is what kind of data constitute this raw material and what happens to the one particular source of this material. In the case of following the logic of the environmental perspective on access to information, the question would rather be of how the deposits of this raw material are used and what are the potential and ongoing consequences of their usage for the whole community.

The right to access information as it is present in the GDPR can increase transparency in terms of the knowledge of an individual on the actual usage of his or her personal data in the digital economy. However, the form that this legal instrument takes in the GDPR has its limits. Moreover, increasing the transparency does not mean that the subject which is using personal data and shaping the digital environment will be held responsible for their actions by data subject. The accountability in the relation between an individual and data controller or processor depends on the instruments which grant and facilitate access to justice. The following section discusses potential inspiration on this matter – drawn from the environmental law – for the regulation of the digital environment.

IV.5 Access to Justice as an Instrument to Support Accountability

As shown above, certain solutions adopted in environmental law, specifically the EIA, access to information and public participation, may be a source of inspiration for the improvement of the data protection regime. In this section, we would like to propose one further step. The legal instruments create an intertwined system. Access to information and public participation do not on their own provide sufficient

87 See, for example, definition of 'environmental information' in Aarhus Convention, Art 2(3).
88 Aarhus Convention, Art 4.

measures to ensure effective public participation in the processes concerning the environment on all of the stages of the process. They should be completed with legal instruments ensuring access to justice, as illustrated by the norm included in the third pillar of Aarhus convention.

In the context of the natural environment, it has been noted that the commoditisation of natural resources demands the participation of various stakeholders in the decision-making process.[89] What is, however, unique about the environmental law is the position of NGOs and their legal standing in terms of enforcement of the Aarhus Convention rights. The access to justice both functionally completes the participation in the decision-making, and constitutes a right of NGOs on its own. Due to Art 9(2) of the Aarhus Convention, the environmental NGOs, provided they comply with the requirements under national law, should be considered as being 'public concerned'.[90] Moreover, they are granted an automatic right of access to justice:

> Unlike natural or legal persons, NGOs promoting environmental protection always have the status of 'the public concerned' provided that they comply with 'any requirements under national law'. Consequently, NGOs acting for the protection of the environment are deemed (..) to "have an automatic right of access to justice".[91]

Such an approach has been a revolution in terms of the execution of the rights included in the Convention.[92] Its innovatory character may be justified in two ways. On the one hand, it means that the 'voiceless' environment,[93] has been given a representative. Taking action in regard to the protection of the environment itself has become easier. On the other hand, the 'public concerned' also gained a possibility

[89] 'the principles and rules of international law have developed as a result of a complex interplay between governments, non-state actors and international organisations. The extent to which a particular area is subject to legal rules will depend upon pressure being imposed by non-state actors, the existence of appropriate institutional fora in which rules can be developed, and sufficient will on the part of states to transform scientific evidence and political pressures into legal obligations' – P. Sands and others, *op. cit.*, p. 23.

[90] Aarhus Convention, Art 9(2).

[91] N. de Sadeleer, *op. cit*., pp. 99–100.

[92] 'Since breaches of environmental law are frequently of concern to the population as a whole without any particular persons being singled out, it is frequently very difficult, if not impossible, to enforce environmental law in judicial proceedings on the basis of the traditional rules of *locus standi*. In other words, the "environment has no voice of its own." (...) The purpose of this reform, which is arguably the greatest innovation introduced by the Convention, is to surmount this obstacle by granting such NGOs to bring certain judicial proceedings "on behalf of 'the environment' " – P. Oliver, *op. cit*., pp. 1431–1433.

[93] L. Krämer, *The Environmental Complaint in the EU*, Journal of European Environmental Law and Planning Law 2009, vol. 6, issue 13, p. 25.

of its interest being represented in the judicial proceedings by NGOs. The latter should be also perceived as in important lesson to be learned in the case of the digital environment, as the importance of the collective dimension of data protection and privacy protection has been noted by legal scholars.[94]

In the GDPR, the presence of NGOs has been introduced to a very limited extent. Their access to justice, as implemented in the provisions of Art 80, is based on the mechanisms of representation of data subject interests.[95] The solution which enables not-for-profit bodies, organisations and associations to lodge a complaint independently of a data subject's mandate is facultative for the member states to implement. Therefore, the access to justice in the case of NGOs is – from the perspective of European data protection law – limited to the situations in which the complaint is linked with a particular case, of a particular data subject. There are no possibilities for the NGOs to pursue proceedings which could allow for the broader scrutiny of data collection or processing. When compared to the actual threats posed by the big data-based analysis, it seems that such a solution does not address the main source of potential problems concerning data protection: its extent. The digital environment is not perceived as an environment in this case, but rather as a set of billions of purely individual data processing and decision-making procedures.

The similarity between the digital environment and the natural environment in this regard is striking. Even though the GDPR may to a certain extent empower the users, it does not include measures which could address the collective challenges arising from the development of the digital economy. The complexity and global dimension of the ongoing changes impede the agency of a single individual. Similarly, as in the case of the natural environment, the results of the undertaken projects usually exceed the local context. The notion which could address this globalisation of data protection related challenges, could be stronger involvement of non-profit bodies into the procedures included in the GDPR and granting them with a certain set of rights concerning access to justice: recognising them as a 'public concerned'.

V. Conclusions

When regulating new technologies, analogies seem to enable the expansion of the perspectives of the search for necessary solutions.[96] In the article, we presented the

[94] See L. Taylor, L. Floridi, B. van der Sloot, *op. cit*.

[95] See GDPR, Art 80.

[96] J. H. Blavin, I. G. Cohen, *Gore, Gibson, And Goldsmith: The Evolution of Internet Metaphors in Law and Commentary*, Harvard Journal of Law & Technology 2002, vol. 16, issue 1, p. 268.

grounds which support the claim that the analogy between the digital environment and the natural environment is a fruitful source of ideas for improvements in the data protection regime. If the principle of data minimisation is to be more than just an empty phrase, it is necessary to develop legal instruments which can ensure its enforcement.[97] The vague terminology of the GDPR's data protection principles catalogue should be complemented with legal instruments which would translate the abstract principles into specific provisions forming a set of legal instruments.

Our analysis shows that such a process can be observed in environmental law. We follow M. J. Emanuel's statement that 'in regards to formulating successful privacy protection, there is no reason to reinvent the wheel'[98] and show how specifically the European environmental law could inspire the development data privacy law, vital for the digital environment. The EIA, the right to environmental information and public participation, as well as the right to access to justice, have evolved within last 30–40 years in European law: they have undergone the change from being solely non-specific rules to the fundamental legal instruments of environmental law on their own.[99] This motion, the evolution from roughly formulated rules to the legal instruments being an integral part of the environmental law, provides us with the lessons which could be learned by data protection law from environmental law. It shows the importance of a detailed and thorough examination of which legal instruments and how precisely defined constitute the actual content of the principles.

In the GDPR it is possible to identify certain traces of translating abstract principles into more specific legal instruments. The DPIA, information obligations, and the right to access seem to transmit the goals set for the data protection by design and by default rules (and therefore, data minimisation principle) into more exactly defined legal instruments. However, allowing for the DPIA to remain an internal procedure will hamper the execution of the fundamental data protection principle. Our analysis shows that, for example, a broader and common European list of types of data processing which should be subject to the DPIA, the necessity to include an alternative analysis in the DPIA, the necessity to define conditions concerning consultations and public involvement when conducting the DPIA, the necessity to strengthen the position of the supervisory authority in the process and dissemination of the information on the DPIA. Such elements, which are present in the European environmental law, could provide inspiration for data protection law. In case

[97] Such a claim can be also supported by the experiences collected in the area of environmental law – as described in the article – where, for example, adoption of the EIA Directive served as grounds for achieving common standards of conducting the impact assessments.

[98] M. J. Emanuel, *op. cit.*, 427.

[99] To the extent of perceiving them as procedural principles, see V. P. Nanda, G. Pring, *op. cit.*, pp. 47–68.

of the confrontation of the basic principles of environmental law regarding access to information and public participation with the GDPR's provision, it seems clear that European data protection law – contrary to environmental law – does not contain solutions which would ensure broader and collective access to information. They are focused on the individual. Moreover, the GDPR does not guarantee the collective actors a right of access to justice. The collective character of the risks posed by the rapid development of the data-based economy could direct our attention to such procedural guarantees as a legal instrument, the presence of which could enrich the possibilities of the public concerned in the digital environment to execute its rights.

The first step necessary to pursue the analogy presented in the article is the understanding of the real impact of the digital environment – not only on individuals, but also on whole communities, or societies. The number of stories in which such a collective dimension of data protection related issues is present grows, examples being the Cambridge Analytica scandal, or discriminatory mechanisms applied in automated decision-making procedures.[100] The question of whether we will be ready to acknowledge the importance of the collective interests in the digital environment remains open. Some traces in the GDPR support the belief that, to a limited extent, the idea of data protection as a collective issue has been acknowledged by the lawmakers. However, further steps would have to be made in order to ensure its more comprehensive adoption. Environmental law seems to be there to – if not to inspire the perfect solutions – then at least provide the lessons learned during its development.

Abstract

The goal of the article is to examine the similarities between the legal instruments adopted in the area of data protection law (fundamental for the digital environment), and the legal instruments adopted in the area of environmental law (fundamental for the natural environment). We identify the legal instruments in the General Data Protection Regulation which resemble ones used in environmental law, namely impact assessment and access to information. In order to provide new insight into the regulation of new technologies, we trace back the history of these instruments' development in EU and international law and indicate their elements which have developed in environmental law and have not been transmitted to data protection law. The article constitutes an input into the broader discussion on modes

[100] For more on this issue in Europe, see AlgorithmWatch, Bertelsmann Stiftung, and Open Society Foundations, *Automating Society. Taking Stock of Automated Decision-Making in the EU*, 2019, source: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/001-148_AW_EU-ADMreport_2801_2.pdf.

of new technologies regulation and the questions raised by the broadening scope of data collection and processing, which affects the (digital) environment we live in.

Key words: access to information, access to justice, impact assessment, data protection by design and by default, data minimisation, General Data Protection Regulation

Kiedy środowisko staje się cyfrowe. Co ma RODO wspólnego z prawem ochrony środowiska? Streszczenie

Celem artykułu jest zbadanie podobieństw pomiędzy instrumentami prawnymi przyjętymi w ramach prawa ochrony danych osobowych (kluczowego dla środowiska cyfrowego) i instrumentami prawnymi przyjętymi w ramach prawa ochrony środowiska (kluczowego dla środowiska naturalnego). Identyfikujemy instrumenty prawne w Ogólnym rozporządzeniu o ochronie danych osobowych, które przypominają te pojawiające się w prawie ochrony środowiska, czyli ocenę skutków oraz dostęp do informacji. W celu przedstawienia nowej perspektywy na regulację nowych technologii omawiamy historię rozwoju tych instrumentów w prawie UE oraz międzynarodowym oraz wskazujemy te ich elementy, które zostały rozwinięte w prawie ochrony środowiska i nie zostały przeniesione do prawa ochrony danych osobowych. Artykuł stanowi wkład w szerszą dyskusję dotyczącą sposobów regulacji nowych technologii i pytań, które pojawiają się w związku z rozszerzającym się zakresem zbierania i przetwarzania danych, wpływających na (cyfrowe) środowisko, w którym żyjemy.

Słowa kluczowe: dostęp do informacji, dostęp do wymiaru sprawiedliwości, ocena skutków, ochrona danych w fazie projektowania i domyślna ochrona danych, zasada minimalizacji danych, Ogólne rozporządzenie o ochronie danych osobowych

Funding: The input of Joanna Mazur to the article was prepared as a part of the grant project 'Automated decision-making versus prohibition of discrimination in the European law' – funded by the National Science Centre, Poland: Project number 2018/29/N/HS5/00105.