sciendo

Automated Decision-Making and the Precautionary Principle in EU Law[1]

Joanna Mazur

Faculty of Law and Administration,
University of Warsaw
ul. Wybrzeże Kościuszkowskie 47,
Warsaw 00-347, Poland
E-mail: j.mazur@wpia.uw.edu.pl

Abstract: *The article is predicated upon the allegation that there is a similarity between the scientific uncertainty linked to the hazard which human interventions pose to the natural environment and the hazard which the development of automated decision-making techniques poses to certain aspects of human lives in the digital environment. On the basis of this allegation, the analysis examines the similarities between the European environmental law, which is crucial for the natural environment, and the European data protection law, which is fundamental for the digital environment. As there are measures already adopted by the data protection law from the environmental law, such as impact assessments and the right to access information, the main hypothesis of this analysis is to consider whether there are further inspirations for the development of European data protection law which could be drawn from environmental law, regarding the scientific uncertainty which is common to these two areas of regulation. The article examines a legal measure, namely, the precautionary principle, as the conjectural response to the challenges linked to the development of the new technologies. The experiences collected in the area of environmental law concerning the precautionary principle are analysed as a source of lessons to be learned concerning the regulatory measures adopted in order to deal with scientific uncertainty, not only in the natural environment, but also in the digital one.*

[1] This research was supported by National Science Centre, Poland, Project no. 2018/29/N/HS5/00105 titled 'Automated decision-making versus prohibition of discrimination in the European law'.

Keywords: *access to information, automated decision-making, digital environment, European data protection law, European environmental law, GDPR, precautionary principle*

1. Introduction

Automated decision-making has an increasing impact on individuals, communities, and societies as they are implemented in the areas crucial for human life, e.g., access to justice or public services (AlgorithmWatch, 2019). Their effectiveness does, however, come at certain price: the automatisation often decreases the transparency of the adopted solutions (i.a. Burrell, 2016; Noto La Diega, 2018). Not only certain individuals may not understand why they were subjected to a certain decision, but also there appear difficulties in grasping the overall impact that digitalised solutions have on the societies.

The European Union (EU) is an active actor in the area of combating challenges rising from digitisation (Nyman-Metcalf & Papageorgious, 2018, pp. 8–9) and more specifically, automated decision-making. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) includes regulatory measures to cope with the threats posed by the effects of implementing automated decision-making solutions. This article is an attempt to analyse the possible inspirations for further development of these regulatory measures. The hypothesis of the article is that the precautionary principle—as developed in the European environmental law—constitutes a measure which may support regulation of the activities performed not only in the natural environment, but also in the digital one, in the case of facing unknown challenges and situations in which there is a lack of scientific evidence. It results from the allegation that there is a similarity between the hazard that human interventions pose to the natural environment and the hazard that the development of automated decision-making techniques poses to the certain aspects of human lives. A lack of scientific certainty and predictability is a common characteristic of these hazards. For this reason, it might be useful to compare what has been assessed as being either effective or ineffective in other areas of regulation which were affected by such a dilemma.

In order to examine this hypothesis, the article is structured as follows. Section 2 briefly describes the inefficiencies of the EU's regulatory framework concerning automated decision-making in the light of the problem of scientific uncertainty. Section 3 of the article introduces grounds for comparing the European data protection law (fundamental for digital environment) to the

European environmental law (fundamental for the natural environment). Section 4 examines the main hypothesis of the article, using the Commission's guidelines concerning the measures which are adopted in order to apply the precautionary principle in practice (Communication COM(2000) 1 final). It explores the possibilities to find an inspiration for the regulation of the digital environment regulation drawn from the regulation of the natural environment. Section 5 concludes. The research methodology used is formal legal analysis, and dogmatic analysis.

2. Automated decision-making regulation in the GDPR and scientific uncertainty

The term automated individual decision-making appears in the GDPR, as the EU regulatory framework defined the boundaries of the possibilities to use automated individual decision-making by the implementation of Article 22 to the GDPR. It prohibits taking decisions which produce legal or similarly significant effects for the individual solely in automated way (Article 29 Data Protection Working Party, 2017a, p. 19). However, the actual impact of this provision on the usage of automated decision-making development is not yet covered by jurisprudence and is already questioned in the scholarly literature (Wachter, Mittelstadt & Floridi, 2017). Firstly, the issue of the possible interpretation of terms such as "solely", "decision", or "legal or similarly significant effects" appears (Selbst & Powles, 2017; Brkan, 2019). Secondly, there are exceptions to the overall prohibition of automated decision-making allowed by Article 22(2) of the GDPR, namely: data subject consent, contractual obligations, and mandatory laws (analysed in detail by Bayamlıoğlu, 2018). Due to these uncertainties and limitations of the right not to be subjected to automated decision-making processes, there are some doubts as to whether the GDPR addresses challenges posed by the unpredictability of the automated decision-making solutions.

Additionally, according to Articles 13(2)f, 14(2)g, and 15(1)h of the GDPR, in case of automated decision-making, the data subject should receive meaningful information on the logic involved in the process. This right has been called 'right to explanation' in the relevant literature (Goodman & Flaxman, 2016). The provisions have been included in the articles which form a catalogue of information which should be given to a data subject where personal data is collected from the data subject, where personal data has not been obtained from the data subject, and as an element of the right to access. This involves

information on the existence of automated decision-making, including profiling, as defined in Article 22. At least in those cases, the data subject should receive meaningful information about the logic involved in the processing, information on the significance of the processing, and information on the envisaged consequences of the processing for him or her. However, the very existence of the right to explanation in the GDPR is a subject of wide academic discussion (for works against its existence, see Wachter, Mittelstadt & Floridi, 2017; for its existence, see Goodman & Flaxman, 2016; Malgieri & Comandé, 2017; Selbst & Powles, 2017), due to a number of doubts concerning the interpretation of these provisions. They raise as many questions as Article 22, for example: What kind of information on the logic involved should the data subject be provided with? What should be done if the logic involved in making a certain decision is unclear not only for the data subject, but also for the data controller?

Due to the lack of the uniform approach towards these issues, there are reasons to be concerned. Considering the difficulties concerning the explainability of automated decision-making (Edwards & Veale, 2017), it is questionable whether the provisions of GDPR might be perceived as feasible solutions to the problems which can be observed on the horizon. Automated decision-making, in itself, may decrease the transparency of the evaluation process and, therefore, blur the reasons behind certain decisions (Zalnieriute, Moses & Williams, 2019). The involvement of machine learning and deep learning technologies in the process of automated decision-making strengthens these tendencies. Doubts concerning the predictability and foreseeability of making the decisions using these technologies are commonly raised (Scherer, 2016; Burrell, 2016). At the same time, one of the goals of implementing automated decision-making is to grant these types of solutions a certain level of autonomy. The purpose of automation of the decision-making procedures includes enabling algorithms to achieve more effective results compared to the same activities performed by human actors. In order to do so, it is necessary to allow programmed tools to analyse data and—in the most technologically advanced scenarios—learn from them.

While performing this task, discrepancies between the final outcomes and the creators' intentions may appear. This can be the result of, among others, the data used by the algorithms, the unpredictability of the interaction between the developed tool and the data it uses for its advancement, and also due to the lack of understanding as to how exactly the algorithm processes and interprets data (Burrell, 2016; Noto La Diega, 2018, p. 10). The question appears as to what an extent such unpredictability should be allowed to make decisions concerning an individual. The solutions of automated decision-making introduced in various

areas of life in European countries show that the number of policies which are influenced by the development of automated decision-making systems, sometimes fuelled by technologies based on machine learning, is growing.

One of the solutions to this deadlock, which is presented in the literature in defence of the provisions concerning automated decision-making as it is implemented in the GDPR, is the interpretation of relevant articles both by the courts and supervisory authorities in the Member States from the human rights perspective. This refers to such elements of the provisions as the 'legal effect', which from the human rights perspective could refer to any limitation to, for example, the right to health (Malgieri & Comandé, 2017, p. 252), or to the meaning of the term 'meaningful information', which from the human rights perspective should be interpreted broadly (Selbst & Powles, 2017). These concepts allow the addressing of certain inefficiencies of the GDPR due to the broad interpretation of selected terms. However, they do not seem to answer the broader question of the threats posed by the use of the automated decision-making as one of the factors which shapes the digital environment. Firstly, on the basis of the GDPR's provisions, there are still possibilities for data controllers to perform data processing and automated decision-making, for example, on the basis of the consent of the data subject, the results of which will be hard to predict and potentially harmful. Secondly, the provisions do not address the results which have significant effects not only on an individual, but on the communities or the citizens of particular state. Thirdly, regulation of automated individual decision-making, as adopted in the GDPR, does not address the questions arising from the lack of foreseeability of such solutions.

The uncertainty of the results when performing automated decision-making—especially using machine learning tools—in the digital environment is similar in character to undertaking certain projects in the natural environment. What links the challenges of the methods of automated decision-making for data protection and the challenges of the projects which have an impact on the natural environment are their potentially severe consequences for the individuals, communities, and societies as a whole. What must be noted is that the unpredictability of automated decision-making taking place in the digital environment may bring results which seriously affect the functioning of individuals, and even societies, in the physical world. When we consider this type of unpredictability in the areas of the environment and the public health protection, we reach for the precautionary principle. Can this also be a case for the digital environment?

3. What is environmental about data protection law?

It must be noted that there are certain elements of the GDPR, as the most important EU legal act concerning data protection, which resemble the mechanisms referring to the access to information in environmental law: different forms of the right to information, and the impact assessment. Considering different forms of the right to information: firstly, there is information which should be provided to the data subject where personal data is collected from the data subject (Art. 13 of the GDPR) and where personal data has not been obtained from the data subject (Art. 14 of the GDPR). This constitutes the right to receive information. Moreover, the information obligations which are the conditions to consider the consent as informed according to the GDPR (Art. 4(11), recitals 32 and 42 of the GDPR) should be considered as a separate information obligation (and from the perspective of a data subject, an element of the right to receive information). In the context of this article it has to be noted that even though—according to the guidelines of Article 29 Working Party—the catalogue of the information which should be provided in order to consider consent as informed is narrower than the obligation set in Articles 13–14 (Art. 29 Data Protection Working Party, 2017b, p. 15), it still includes information about the use of the data for automated decision-making in accordance with Article 22(2) of the GDPR.

Secondly, another right which is a kind of right to information—the right to access—refers to the further stages of the data processing. The right to access, as defined in Article 15 of the GDPR, may provide the grounds for the availability of information on personal data processing for the data subject *ex post*, after making automated decision and on specific requests of data subjects (Malgieri & Comandé, 2017, p. 246). This allows expanding the concept of the right to information in the area of data protection law. It seems to cover the whole timeline of the data processing: from the moment it is intended (information obligation), to the collection of consent (informed consent), to the moment the automated decision was made (right to access).

Thirdly, in such a general framework of the right to information as shaped by the GDPR, the inclusion of the widely discussed right to explanation in the GDPR (see the references above), is *de facto* a discussion concerning a unique kind of right to information. What is important to note is the difference between the inclusion of the information on automated decision-making taking place in the catalogue of information included in Articles 13–15 of the GDPR and in the guidelines of Article 29 Data Protection Working Party concerning informed consent, and material aspect of the ‘right to explanation’. According to Articles

13–15 of the GDPR, in case of automated decision-making defined in Article 22, the data subject should be provided with meaningful information on the logic involved in the processing: so, information not only about the automated decision-making that takes place, but also about the logic involved. The right to receive such meaningful information constitutes a right to access information, within the catalogue of the information to which the data subject should be allowed access.

Fourthly, another specific kind of right to information in the GDPR has been implemented by Article 34 which obliges the data controller to communicate the breach of personal data to the data subject. The obligation is limited to the situations in which the data breach may result in a high risk to the rights and freedoms of natural persons. The data controller is obliged to describe the data breach in clear language. The information which the data subject should receive includes: (1) contact details of the data protection officer or other contact point where more information can be obtained; (2) the likely consequences of the personal data breach; and (3) the measures taken or proposed to be taken by the controller to address the personal data breach (Art. 34 of the GDPR). The obligation to provide the data subject with information on the data breach should be considered—similarly to the right to explanation—as a measure which is *de facto* a specific kind of right to information.

The fifth element of the GDPR which constitutes a form of a right to information, is the right to data portability. The right to data portability refers not to the processing of the data, but to the processing of personal data—which can be perceived as information—itself. Its main function is to allow the data subject to receive the personal data concerning him or her which he or she has provided to a controller, in a structured, commonly used and machine-readable format. Article 20 of the GDPR refers solely to the situations when the processing is automated and based on contract or consent. The right to data portability allows the data subject, technically, not to rely on one data controller, but to be able to move to a competitor without facing the problem of uploading all of one's data again. It should guarantee a more equal position between the data subject and the data controller and expands the scope of information which the data subject should be able to receive. However, it does not allow assessment of what kind of information has been drawn from this data by the data controller.

Next to the right to information, another regulatory measure developed in environmental law and implemented in the GDPR is impact assessment (this fact was noted by de Hert, 2017, p. 174; Binns, 2017, p. 23). The measure addresses the challenges linked to the processing which is likely to result in a high risk to

the rights and freedoms of natural persons due to its nature, scope, context and purposes (Art. 35(1) of the GDPR). Data protection impact assessment (DPIA) should be conducted in two types of situations. Firstly, if one of the conditions directly enumerated in the GDPR is taking place, among which is 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 (Art. 35(3)a). Thus, DPIA refers to the automated decision-making described in Article 22. Secondly, the supervisory authorities in the Member States should prepare lists of the types of processing which should be subject to the DPIA. This shows that DPIA serves as a tool which should allow mitigating risks resulting from—among other things—automated decision-making. What should be noted, however, is that according to the GDPR the involvement in the process of preparing and discussing DPIA is limited to a very narrow range of bodies (data controllers and, possibly, according to Article 36, supervisory authorities), and there is no obligation to publish its result (Article 29 Data Protection Working Party, 2017c, p. 18). The data subjects or their representative may be involved in the process only "where appropriate" (Art. 35(9) of the GDPR). Therefore, the implementation of DPIA to the GDPR seem to improve the situation of the data subject only to a very limited extent.

These examples illustrate that there are some indications in the European data protection law, fundamental for the digital environment, which show that the conceptualisation of the digital environment as related to the natural environment is present in the regulatory dimension. The implementation of specific regulatory measures known from the environmental law, namely different forms of the right to information and the impact assessment (DPIA) to the GDPR raises the question: is there anything else that the environmental law has to offer in order to improve the data protection law?

4. The precautionary principle for the digital environment

As explained in Section 2 of the article, there is a certain level of scientific uncertainty concerning automated decision-making. The potential harm that automated decision-making may cause is relevant not only for individuals but also for whole groups or even societies. These two types of hazard are created by the spreading of automated decision-making: unpredictability and the consequences which reach far beyond an individual are not fully addressed in

the GDPR. They do, however, resemble the threats posed by certain initiatives which have an impact on the natural environment. Just like they, their effects are sometimes impossible to foresee, and their potentially harmful character has an impact on whole groups of people.

One of the answers which has been adopted to meet this sort of challenge in the environmental law is the precautionary principle. The meaning of the precautionary principle can be summed up as the necessity to consider values such as the protection of the environment as priorities when there is a lack of scientific evidence concerning the results of a certain action. After less than a decade of its development in international law (Sands *et al.*, 2012, pp. 217–228), in 1992, the precautionary principle was implemented in the Maastricht Treaty, initially in relation to the action on the environment: "Community policy on the environment […] shall be based on the precautionary principle" (Art. 130r(2) of the Treaty on European Union).[2] The Article provided grounds for a number of CJEU judgments which addressed the question of the precautionary principle meaning in the EU law, for example *United Kingdom v Commission* ([1998], p. 02265) or *National Farmers' Union and Others* ([1998], p. 02211).

The CJEU's interpretation of the precautionary principle is often summed up with the phrase: "where there is uncertainty as to the existence or extent of risks to human health, protective measures may be taken without having to wait until the reality and seriousness of those risks becomes fully apparent" (enumeration of the relevant case law, see de Sadeleer, 2006, p. 142). This explanation of the precautionary principle by the CJEU shows the expansion of the principle's application from the protection of the environment to the protection of public health. As stated in the case *Alpharma Inc. v. Council of the European Union* ([1999], p. 02027): "requirements linked to the protection of public health should undoubtedly be given greater weight than economic considerations". Due to this broadened scope of the meaning of the precautionary principle in EU law, its essence may be summed up as "a general rule enshrined in European law which gives precedence to health (and similar) concerns over economic interests in cases of uncertainty" (Ladeur, 2003, p. 1455).

As the precautionary principle generates much disagreement and discussion concerning its meaning and effect in EU law (i.a. van Asselt & Vos, 2006), the purpose of this section is not to engage in this debate but to focus on the consideration of the precautionary principle application to the digital environment. Therefore, there are two questions which should be discussed:

[2] Currently, Consolidated version of the Treaty on the Functioning of the European Union (2012), *OJ* C 326/47, Art. 191(2).

Does the scope of the precautionary principle application in EU law allow claiming that there are situations in which automated decision-making should be considered as subject to analysis in terms of its accordance with the precautionary principle? And: What are the formal aspects of the requirements of applying the precautionary principle, as established in the Commission's communication on the precautionary principle (Communication COM(2000) 1 final), which might be considered as an inspiration to adopting the relevant solutions to data protection law concerning automated decision-making?

Considering the scope of application of the precautionary principle, initially the value which it was supposed to protect was the environment (for example, in the area of wildlife conservation or chemical management). Such an approach does not seem to allow the simple transition of the precautionary principle to the digital environment. Technically it is possible to adopt characteristics of the digital environment which should be protected (e.g., network neutrality). However, it seems too far reaching and if it is to be considered, should be approached from a more philosophical perspective (Pieters & van Cleeff, 2009, p. 52).

However, the scope of application of the precautionary principle was expanded to the protection of public health (de Sadeleer, 2006, p. 142). The application of the precautionary principle in the area of public health protection took place in CJEU case-law (see above), and was confirmed by the Commission's communication (Communication COM(2000) 1, p. 19). The necessity to apply the precautionary principle in the area of public health indicates its possible relation to automated decision-making. The example is automated systems, such as RiskER, which serve the goal of predicting the risk of hospitalisation (AlgorithmWatch, 2019, p. 89). The aim of bringing up this example is not to question their usefulness in supporting the prediction of risk of hospitalisation based on data analysis. It is rather to stress the necessity of careful scrutiny if there are no "side effects" of such automated decision-making, for example, if criteria such as ethnicity or gender do not hamper the accuracy of the predictions. If the precautionary principle is about prioritising, for example, health over economic gain and if the results of the initiative are impossible to foresee, are threats posed by the immaterial automated decision-making systems different than the material substances which have a harmful impact on human health? Such a broad perspective for relationship between automated decision-making and public health is the first inspiration which can be drawn from environmental law into the European regime governing the digital environment, especially in the area of data protection.

This conclusion brings us to the second question: If the precautionary principle could be applied to the selected cases of automated decision-making, which may have a harmful effect on public health, what are the formal requirements which should be fulfilled in such a case? In its communication concerning the precautionary principle, the Commission presents the principle as "politically accepted […] risk management strategy in several fields" (Communication COM(2000) 1, p. 8) and lists four steps which should be taken when applying the principle. As summarised by Fisher (2002),[3] the steps are: (1) risk assessment which reveals the potential risk and lack of scientific evidence or uncertainties concerning the risk; (2) decision to act or not to act, which should be based on the political decision concerning the level of acceptable risk; (3) transparent and inclusive process of assessing the consequences of different forms of action and inaction; and (4) decision in relation to what measures should be taken (Fisher, 2002, pp. 11–12). Such an approach where the application of the precautionary principle is preceded by a risk assessment has been criticised by Sadeleer, who claims that "the precautionary principle is located within the broader context of risk analysis, which comprises a two-step process: risk assessment and risk management" (de Sadeleer, 2006, p. 146) and therefore:

> *from a legal point of view, nothing precludes that the risk assessment stage has to be carried out in accordance with the obligations stemming from the precautionary principle […]. Indeed, in order to deal effectively with uncertainty, ambiguity, and ignorance, assessors should apply precaution at an early stage.* (de Sadeleer, 2006, p. 148)

These conflicting opinions on the application of the precautionary principle show two possibilities of its usage in the area of data protection. Firstly, it could potentially become an indication for the early stage of automated decision-making solutions' development. However, there are hardly any reasons to believe that such an approach might be supported by the current data protection regulatory framework. What may become a starting point for a discussion of the precautionary principle application on the early stages of automated decision-making development, is the implementation of the data protection by design and by default to Article 25(1) of the GDPR. Such a requirement might be an indication of the possibility to apply the precautionary principle when determining the means for processing—which is the earliest stage that it could be applied.

[3] The reason to turn to the literature from the early 2000s is that the precautionary principle seems to have been a hot topic in the first decade of the 21st century, while not being much explored since then in academic discourse.

Secondly, the application of the precautionary principle in the area of data protection law might be considered as an indication of how to conduct a DPIA. According to Article 35(1) of the GDPR, the DPIA should be performed in cases of processing which are likely to result in a high risk to the rights and freedoms of natural persons. Therefore, the condition of revealing the potential risk (Step 1 of the precautionary principle application) is met. Secondly, the DPIA should be performed prior to the processing, which implies the necessity to make a decision, based on the acceptable risk level, to act or not to act (Step 2). The provisions concerning DPIAs also include the description of the decision concerning what measures should be taken (Step 4).

What might become an inspiration drawn from the application of the precautionary principle—as defined by the Commission's communication—to the data protection law, is Step 3. The Articles concerning DPIAs (Art. 35–36 of the GDPR) do not define the transparent and inclusive process of assessing the consequences of different forms of action and inaction (Step 3). The procedures established in the GDPR involve the data controller and may involve the supervisory authority. Meanwhile, the data subject should be consulted "where appropriate" (Art. 35(9) of the GDPR). This vague description does not guarantee the actual involvement of various stakeholders in DPIAs. Therefore, the second proposal of the improvement of data protection law on the basis of the experiences drawn from the environmental law is to increase transparency and inclusiveness of the process of assessing the consequences of different forms of action and inaction concerning automated decision-making.

5. Conclusions

The similarities between the nature of challenges faced in the area of the environmental law and in the data protection law and the resemblance of the legal measures adopted in order to deal with these issues, provide grounds for an examination of another legal measure which was developed in the environmental law. The precautionary principle was meant to regulate the behaviour when facing the risks, the nature of which is not yet fully known. As the risks posed by automated decision-making share this characteristic with some initiatives undertaken in the natural environment, the precautionary principle may serve as a tool which could support the further development of data protection law. It could become a guideline for tackling the scientific uncertainty by the regulation of the digital environment. As the results of the analysis show, if the automated

decision-making solutions were to pose a serious risk for public health or a high level of an unpredictability if applying these solutions in the policies referring to the protection of health, it might be possible to apply the precautionary principle as a legal measure to address the identified risks.

Moreover, on the basis of the guidelines concerning the application of the precautionary principle in EU law, it is reasonable to claim that it could be treated as a guideline for conducting a DPIA. The first condition concerning the application of the precautionary principle in EU law would be automatically fulfilled as a DPIA should be conducted in cases of the risks resulting from data processing, including using automated decision-making. The inspiration which can be drawn from the guidelines concerning the application of the precautionary principle in EU law refers to the transparency and inclusiveness of the process assessing the consequences of different forms of action and inaction. In the GDPR such possibilities are very limited, and the interpretation of the regulation's provisions could benefit from the experiences collected in environmental law in this regard.

The practical implementations of the research could include strengthening the position of non-governmental actors in terms of receiving the relevant information on DPIAs. It is possible, within the existing regulatory framework, to create expert bodies which could support consultations of DPIA with supervisory authorities on the national level. When a data controller decides to consult a supervisory authority, such an expert body could be involved in the search of the relevant solution. Such an expert body could also cooperate with non-governmental organisations and academics, which might shift the focus of the debate onto the ethical aspects of automated decision-making. Moreover, during consultations, alternative options could be considered—as is the case when conducting environmental impact assessment. Thus, even though such a requirement concerning DPIAs in not mentioned in the GDPR, it could become a measure used in assessing the level of data protection implemented in particular systems or solutions.

Finally, it should be noted that the measures which are to be taken as the results of the precautionary principle application do not need to have a regulatory character: they might include, for example, research programmes (Fisher, 2002, p. 11). Due to this, the interpretation presented in the article may not hamper innovativity. Instead, it can provide impulses to pursue further research and improve the existing technologies in order to support the development of a fairer digital environment.

Joanna Mazur is a PhD candidate at the Faculty of Law and Administration, University of Warsaw, and a researcher in DELab UW. The article is part of the project 'Automated decision-making versus prohibition of discrimination in the European law', funded by National Science Centre, Poland, under grant no. 2018/29/N/HS5/00105.

References

AlgorithmWatch (2019), *Automating Society. Taking Stock of Automated Decision-Making in the EU*, A report by AlgorithmWatch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations, Berlin: AW AlgorithmWatch gGmbH. Retrieved from https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/001-148_AW_EU-ADMreport_2801_2.pdf [accessed 8 Aug 2019]

Alpharma Inc. v. Council of the European Union, Order of the President of the Court of First Instance of 30 June 1999 (Interim Measures) [1999], ECR II, T-70/99, 30.6.1999.

Article 29 Data Protection Working Party (2017a), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018*, WP 251 rev. 01.

Article 29 Data Protection Working Party (2017b), *Guidelines on Consent under Regulation 2016/679*, WP 259, 28.11.2017.

Article 29 Data Protection Working Party (2017c), *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, 4.4.2017.

Bayamlıoğlu, E. (2018), 'Transparency of automated decisions in the GDPR: an attempt for systemisation.' Retrieved from https://ssrn.com/abstract=3097653 [accessed 8 Aug 2019]. https://doi.org/10.2139/ssrn.3097653

Bayamlıoğlu, E. & Leenes, R. (2018), 'The 'rule of law' implications of data-driven decision-making: a techno-regulatory perspective,' *Law, Innovation and Technology*, vol. 10, no. 2, pp. 295–313. https://doi.org/10.1080/17579961.2018.1527475

Binns, R. (2017), 'Data protection impact assessments: a meta-regulatory approach,' *International Data Privacy Law*, vol. 7, no. 1, pp. 22–35. https://doi.org/10.1093/idpl/ipw027

Brkan, M. (2019), 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond,' *International Journal*

of Law and Information Technology, vol. 27, no. 2, pp. 91–121. https://doi.org/10.1093/ijlit/eay017

Burrell, J. (2016), 'How the machine "thinks": Understanding opacity in machine learning algorithms,' *Big Data and Society*, vol. 3, no. 1, pp. 1–12. https://doi.org/10.1177/2053951715622512

Communication COM(2000) 1 final from the Commission on the precautionary principle, 2.2.2000.

Consolidated version of the Treaty on the Functioning of the European Union, *OJ*, C 326, 26.10.2012, pp. 47–390.

de Hert, P. (2017), '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*, vol. 3, no. 2, pp. 160–179. https://doi.org/10.21552/edpl/2017/2/6

de Sadeleer, N. (2006), 'The precautionary principle in EC health and environmental law,' *European Law Journal*, vol. 12, no. 2, pp. 139–172. https://doi.org/10.1111/j.1468-0386.2006.00313.x

Edwards, L. & Veale, M. (2017), 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for,' *Duke Law and Technology Review*, vol. 16, no. 1, pp. 18–84. https://doi.org/10.31228/osf.io/97upg

Fisher, E. (2002), 'Precaution, precaution everywhere: developing a "common understanding" of the precautionary principle in the European Community,' *Maastricht Journal of European and Comparative Law*, vol. 9, no. 1, pp. 7–28. https://doi.org/10.1177/1023263X0200900102

Goodman, B. & Flaxman, S. (2016), 'European Union regulations on algorithmic decision-making and a "right to explanation",' in *2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)*, New York. Retrieved from https://arxiv.org/pdf/1606.08813.pdf [accessed 9 Aug 2019]

Ladeur, K.-H. (2003), 'The introduction of the precautionary principle into EU law: a pyrrhic victory for environmental and public health law? Decision-making under conditions of complexity in multi-level political systems,' *Common Market Law Review*, vol. 40, pp. 1455–1479.

Malgieri, G. & Comandé, G. (2017), 'Why a right to legibility of automated decision-making exists in the General Data Protection Regulation,' *International Data Privacy Law*, vol. 7, no. 4, pp. 243–265. https://doi.org/10.1093/idpl/ipx019

National Farmers' Union and Others [1998], *The Queen v. Ministry of Agriculture, Fisheries and Food and Commissioners of Customs & Excise, ex parte National Farmers' Union and Others*, ECR I, C-157/96, 5.5.1998.

Noto La Diega, G. (2018), 'Against the dehumanisation of decision-making – algorithmic decisions at the crossroads of intellectual property, data protection, and freedom of information,' *Journal of Intellectual Property, Information Technology and*

E-Commerce Law, vol. 9, no. 3, pp. 3–34. https://doi.org/10.2139/ssrn.3135357

Nyman-Metcalf, K. & Papageorgiou, I. F. (2018), 'The European Union digital single market—challenges and impact for the EU Neighbourhood states,' *Baltic Journal of European Studies*, vol. 8, no. 2(25), pp. 7–23. https://doi.org/10.1515/bjes-2018-0013

Pieters, W. & van Cleeff, A. (2009), 'The precautionary principle in a world of digital dependencies,' *Computer*, vol. 42, no. 6, pp. 50–56. https://doi.org/10.1109/MC.2009.203

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) (Text with EEA relevance) (GDPR), *OJ*, L 119, 4.5.2016, pp. 1–88.

Sands, P.; Peel, J.; Fabra, A. & MacKenzie, R. (2012), *Principles of International Environmental Law*, New York: Cambridge University Press.

Scherer, M. U. (2016), 'Regulating artificial intelligence systems: risks, challenges, competencies, and strategies,' *Harvard Journal of Law and Technology*, vol. 29, pp. 353–400. https://doi.org/10.2139/ssrn.2609777

Selbst, A. D. & Powles, J. (2017), 'Meaningful information and the right to explanation,' *International Data Privacy Law*, vol. 7, no. 4, pp. 233–242.

Treaty on European Union (Maastricht Treaty), *OJ*, C 191, 29.7.1992, pp. 1–112. https://doi.org/10.1093/idpl/ipx022

United Kingdom v. Commission [1998] *United Kingdom of Great Britain and Northern Ireland v. Commission of the European Communities*, ECR I, C-180/96, 5.5.1998.

van Asselt, M. B. A. & Vos, E. (2006), 'The precautionary principle and the uncertainty paradox,' *Journal of Risk Research*, vol. 9, no. 4, pp. 313–336. https://doi.org/10.1080/13669870500175063

Wachter, S.; Mittelstadt, B. & Floridi, L. (2017), 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation,' *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99. https://doi.org/10.1093/idpl/ipx005

Zalnieriute, M.; Moses, L. B. & Williams, G. (2019), 'The rule of law and automation of government decision-making,' *The Modern Law Review*, vol. 82, no. 3, pp. 425–455. https://doi.org/10.1111/1468-2230.12412