e. publica
public law journal

The challenges of the GDPR in the era of Artificial Intelligence: what can we expect from the future?

Diana Camões

Vol. 11 No. 3
Dec 2024
e-publica.pt

ISSN 2183-184x

Com o apoio de:

Fundação para a Ciência e a Tecnologia

THE CHALLENGES OF THE GDPR IN THE ERA OF ARTIFICIAL INTELLIGENCE: WHAT CAN WE EXPECT FROM THE FUTURE?

OS DESAFIOS DO RGPD NA ERA DA INTELIGÊNCIA ARTIFICIAL: O QUE PODEMOS ESPERAR DO FUTURO?

DIANA CAMÕES[1]
Portuguese Parliament
Portugal
diana.camoes@hotmail.com
ORCID 0000-0001-8827-007X

Abstract: Over the past years, the development of Artificial Intelligence has changed the world, leading to what is known as algorithmic society. Progressively, decisions being adopted by humans started being performed by automated means. This development has had a tremendous impact in the quality of our daily life, as it also raises several challenges, especially regarding the protection of fundamental rights in this digital era. The widespread adoption of new technology created the need to adapt the existent legal framework to these challenges, which led to the Artificial Intelligence Act. Hence, with new regulations being created, it is imperative to reflect about the General Data Protection Law Regulation in this time of Artificial Intelligence. This article evaluates how data protection law can adapt itself to these new challenges raised by the algorithmic society, especially concerning the protection of data subjects.

Keywords: General Data Protection Regulation; artificial intelligence; digital rights; automated decision-making; digital era

Resumo: Nos últimos anos, o desenvolvimento da Inteligência Artificial mudou o paradigma mundial, levando ao surgimento da sociedade algorítmica. Progressivamente, as decisões que eram adotadas por seres humanos começaram a ser efetuadas por meios automatizados. Este desenvolvimento teve um tremendo impacto na qualidade do nosso dia a dia, tendo levado ao surgimento de diversos desafios, especialmente no que respeita à proteção de direitos fundamentais na era digital. A adoção de novas tecnologias criou a necessidade de se adaptar o atual enquadramento legal, o que levou à aprovação do Regulamento da Inteligência Artificial. Assim, com a criação de novos regulamentos, torna-se imperativo refletir sobre o Regulamento Geral sobre a Proteção de Dados nesta era da Inteligência Artificial. Este artigo avalia como pode o direito da proteção de dados adaptar-se aos novos desafios da sociedade algorítmica, especialmente no que respeita à proteção do titular dos dados.

Palavras-chave: regulamento geral sobre a proteção de dados; inteligência artificial; direitos digitais; decisões individuais automatizadas; era digital

1. Legal Advisor at the Portuguese Parliament. Bachelor's degree in Law at Porto Faculty of Law (Catholic University). Master's degree in International and European Law at Porto Faculty of Law (Catholic University), Postgraduate degree in Data Protection Law at the Private Law Research Center (Lisbon Faculty of Law) and Postgraduate in Digital Services at the Consumer Law Institute and Private Law Research Center (Lisbon Faculty of Law).

1. Introduction

Artificial Intelligence (hereinafter "AI") has played a major role in our society, leading to what is known as "algorithmic society[2]". There has been an ongoing process of implementation of digital technologies in AI, which has contributed to "mediating daily life and society at large" (Gregorio, 2023: 2). Hence, we have witnessed a migration of certain responsibilities and functions from humans to machines (Rubestein, 2021: 750).

Thus, with the recent coming into force of the AI Act[3], which represents a similar milestone as the General Data Protection Regulation[4] (hereinafter "GDPR") in terms of the European Union's legislation, data protection law will have to adapt itself to this new reality.

These two legal frameworks are different and there might exist "areas of tension between objectives and obligations" (Winau, 2023: 124), as they do not share the same scope of application and, as a consequence, do not require the same approach. Nonetheless, we argue that it would be a mistake simply to ignore the importance of the GDPR in the following years in regards to AI, especially in whatever concerns the protection of data subject's digital rights in this modern society.

After all, data protection "is meant to protect people's privacy, identity, reputation, and autonomy" (Watcher, Mittelstadt, 2019: 495) and its importance should not be underestimated[5]. We have witnessed, in respect to Generative AI[6], the European Data Protection Supervisor adopting its first guidelines on AI and personal data for institutions, bodies, offices and agencies[7].

Even though it has been clarified that a relation of complementarity between these two different regulations has to be established, there are areas of tension, which imply the need to adapt the existing regulation to these new challenges[8].

Therefore, this article starts by outlining the situations in which the GDPR will still be applicable to AI systems. On a second note, we analyze article 22. and the need of a change of the regulatory framework or, at least, its interpretation. Third, we evaluate whether article 22 of the GDPR, in this age

2. Reference made by Gregorio (2022: 6). See Pollicino, Gregorio (2022: 4).

3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

5. Paragraph 2 of article 1 of the GDPR clarifies its goal of protecting fundamental rights and freedoms of natural persons and in particular the right to protection of personal data.

6. Generative AI corresponds to a subset of AI that can be used to create new content, including images, text, videos, audio and simulations.

7. European Data Protection Supervisor. Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems. URL: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en (accessed 24/08/2024).

8. As Kaminski, Malgier (2021: 126) recall, "the GDPR has significant implications for algorithmic decision-making" and that is precisely why its role cannot be ignored.

of AI, can constitute a feasible tool in protecting the data subject's digital rights.

Our goal is to demonstrate how Data Protection, especially the GDPR, can still be a useful guide in this era of AI[9], in order to allow the reconciliation of innovation and respect for people's rights. To achieve this goal, is it time to rethink the actual data protection's legal framework? That is what we aim to find out.

2. The GDPR's applicability to AI's systems

The GDPR is applicable to controllers[10] and processors[11] that process personal data in the context of activities of an establishment in the Union[12], regardless of whether the processing takes place in the EU[13] or not and when the processing activities are related to the supply of goods or services and the monitoring of data subjects' behaviors, as far as it takes place in the EU[14].

One important note is that the GDPR tends to be applicable regardless of the processing occurring wholly or partly by automated means[15]. The legislator did not present a definition of "automated means", which is understandable, because a precise definition would lead the article to be out of date (Cordeiro, 2021: 67) due to the development of new technologies.

For this reason, in order for the GDPR to be applicable to AI's systems, a processing of personal data will have to occur. The notion of processing, as foreseen on the GDPR[16], is broad and "describes almost all operations likely to involve personal data" (Pollicino, Bassini, Gregorio, 2022: 193) and it includes the ones taking place within the context of AI[17]. These Machine

9. See Genderen (2017: 1-15).

10. According to paragraph 7 of article 4 of the GDPR, a controller corresponds to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

11. Paragraph 8 of article 4 of the GPDR. A processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

12. Paragraph 1 of article 2 of the GDPR.

13. Paragraph 1 of article 3 of the GDPR.

14. Subparagraph a), of paragraph 2 of article 3 of the GDPR and subparagraph b), of paragraph 2 of article 3 of the GDPR.

15. Paragraph 1 of article 2 of the GDPR. Barbosa, Félix (2021: 69).

16. According to paragraph 2 of article 4 of the GDPR "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

17. The definition presented by the AI Act of AI system is very similar to the one given by OECD ("Organization for Economic Co-operation and Development"). According to article paragraph 1 of article 3 of the AI Act, an AI system means a "machine-based

Learning systems, which are set to be applicable in the course of analyzing data concerning natural persons, "use and combine that data in order to discover patterns necessary for making decisions or suggestion" (Kesa, Kerikmäe, 2020: 75). Consequentially, and due to the broad definition given by the GDPR, most certainly a processing activity will occur.

Additionally, the key point for its applicability resides on that processing made by the AI system involving personal data, as defined by paragraph 1 of article 4 of the GDPR[18] ("any information relation to an identified or identifiable natural person").

Therefore, it is possible to outline four different scenarios:

i) In some cases, in regards to AI systems, there will be situations where both the AI Act and the GDPR will be applicable. It can be the case, for example, of an AI system intended to be used for the recruitment or selection of natural persons and to evaluate candidates. In this case, not only this system will constitute a High-Risk AI system, in accordance do Annex III of the AI Act[19], as well as it will imply the processing of personal data (for example, names, age, e-mail, phone number and all the information relating to the data subject, which will be the job seeker).

ii) In other scenarios, only the AI Act will be applicable. It can be the case of AI Systems concerning critical infrastructure, which are used as safety components in the management and operation of electricity[20] infrastructure, for example. This will constitute a High-Risk AI System, but it will not involve the processing of personal data[21].

iii) Additionally, it is possible to mention cases where only the GDPR will be applicable. The main example is the usage of an AI System for the sole purpose of scientific research and development, which are excluded from the AI Act's

system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environment".

18. It involves four different elements, namely: (i) any information, ii) relating to, (iii) identified or identifiable and (iv) concerning a natural person. Over the years, the concept of personal data has been well densified not only by ARTICLE 29 WORKING PARTY (2017: 1-19). See, for example, Judgment of 20 December 2017, *Novak*, C-434/16, EU:C:2017:994; Purtova (2018: 40) and Cordeiro (2018: 297-321).

19. Namely article paragraph a) of article 4 of Annex III of the AI Act. It will, as a consequence, have to comply with all the provisions laid down on chapter III of the AI Act.

20. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS has given as an example AI system applied to power plant management. See COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS. Entry into force of the European AI Regulation: the first questions and answers from the CNIL. URL: https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil (accessed 05/08/2024).

21. See article 2 of Annex III of the AI Act.

applicability[22]. Nonetheless, the GDPR will still be applicable, as there will be the processing of personal data.

This can also be the case of AI systems of minimal risks, which are unregulated by the AI Act and a vacuum might be created. To the extent that those systems imply a processing of personal data, the GDPR will be relevant.

iv) Finally, there can be situations where none of the regulations are applicable. It can be the case of AI Systems of minimal risks, which are not covered by the AI Act and that do not imply the processing of personal data. On this matter, it is possible to invoke the example given by CNIL: an AI system used for simulation in a video game[23].

From what we have seen, it is possible to outline that there are several situations where, in regards to AI system's, the GDPR can still play an important role, which will demand rethinking the existent legal framework. One should bear in mind that the GDPR aims to ensure the protection of the fundamental right to privacy and, as a matter of fact, it evolves around the exercise of data subject's rights in regards to the processing of personal data.

3. Automated decision-making – is it time to rethink the legal framework?

Article 22.º of the GDPR is the most important provision in what concerns Automated Decision-Making (ADM), but it cannot be considered a novelty, as the Data Protection Directive[24] had already addressed this topic on article 15. Some see it as a "vivid example of how the Europeans have imposed restrictions on fully automated processing for computational technologies" (Lazcoz, Hert, 2023: 4). Regardless of its tremendous impact, especially having in mind that these type of systems "disrupt traditional concepts of privacy and discrimination" (Watcher, Mittelstadt, 2019: 574), the fact is that it has been almost completely ignored over the years.

Thus, a clear interpretation is due and, regarding these systems, some questions remain controversial: (i) does article 22.º constitute a right or prohibition and (ii) how does the definition of automated decision-making imply human intervention.

3.1. Assessing the nature of article 22

Over the years, there has been an ongoing debate on the nature of article 22, namely to know if this provision should be interpreted as a prohibition of

22. Paragraph 6 of article 2 of the AI Act.

23. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS. Entry into force of the European AI Regulation: the first questions and answers from the CNIL. URL: https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil (accessed 05/08/2024).

24. Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995.

all automated decision-making or, instead, a right of the data subject to object. We shall start by outlining, as we have defended before (Camões, 2024: 44-45), that we interpret it as a prohibition.

The ambiguity of this question is not new. Back then, paragraph 1 of article 15 of Directive 95/46/CE allowed the "right not to be subject of an automated decision". This led some Member States to implement it as a general prohibition[25], while others ended up adopting it as a right that should be exercised[26].

Regardless of this fact, there would not exist any problem if the GDPR had allowed the possibility to end this dilemma. This was not, unfortunately, the case. One should bear in mind that Regulations within the EU become immediately enforced as law in all Member States simultaneously and, contrarily to Directives, it is not necessary any act of transposition to its internal legal order. The GDPR should have contributed to a coherent approach, which was not possible.

According to paragraph 1 of article 22 of the GDPR, "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

Many scholars view it as a right of the data subject (Bygrave, 2020: 531; Thouvenin, Fruh, Henseler, 2022: 183-198; Tosoni, 2021: 145-162; Calvão, 2024: 82; Moniz, 2023: 199; Pinheiro, Gonçalves, 2018, 388; and Kaminski, Urban, 2021: 1978). Following this position would imply defending this as an active right which would make its exercise "solely dependent on the data subject's choice" (Barbosa, Félix, 2021, 72; Costa, 2021, 56)[27].

This position is based on several arguments. First, it is outlined that the wording of article 22 ("*the data subject shall have the right not to be subject*") is clear in ensuring that this is a right of the data subject. In fact, it is taken into consideration the fact that the wording remained essentially unchanged when compared to Article paragraph 1 of article 15 of the Data Protection Directive[28]. Second, it is invoked an argument related to the *travaux préparatoires*. There was an amendment to change the wording of the provision, which would make it clear the existence of a general prohibition[29]. However, the amendment was rejected, which would suggest that this line of interpretation was initially refused. Lusa Tosoni argues that, if there was an intention to create a general ban on profiling, then, "this intention would have left a clear trace in the legislative history of the provision" (2021: 150).

Additionally, it is argued that from a systematic point of view this is the only coherent solution, as article 22 is inserted on chapter III which addresses rights of the data subject. The Hellenic Data Protection Authority ("HDPA"), back in 2021, adopted this line of interpretation on the Case 51/2021. The individual filed a complaint on the grounds that his bank's nuisance phone

25. For example, Belgium, Germany and Austria.

26. Norway, for example.

27. See Silveira (2023: 77).

28. Outlining this point, see Mendoza, Bygrave (2017: 20) and Watcher, Mittelsdat, Floridi (2017: 94-95).

29. Proposal presented by Jan Philipp Albrecht.

calls on debt matters constituted an automated decision-making. The HDPA considered that the data subject failed to present his arguments (namely regarding its applicability under article 22 of the GDPR) and it also considered that the data subject should exercise their rights through the right to object under article paragraph 1 of article 21 of the GDPR[30].

Even though we can understand some of the arguments presented by this line of interpretation, we cannot agree with it. First of all, interpreting article 22 of the GDPR as a right would create an excessive burden on the data subject's part (Barbosa, Félix, 2021: 73; Watcher, Mittelsdat, Floridi, 2017: 95; Rebelo, 2023: 284-285).

Instead, when interpreting article 22 as a general prohibition, they do "not need to act to prevent automated decision-making, but are rather protected by default" (Watcher, Mittelsdat, Floridi, 2017: 95). There is an automatic protection, which in fact reinforces the data subject's protection (Mendoza, Bygrave, 2017: 9-10). It would be contradictory giving the possibility to react the decision (*ex post*), if it was possible to object the decision prior to it being made (*ex ante*) (Camões, 2024: 46)[31].

On the other hand, it is also important to note that this is the only interpretation that is coherent with article paragraph 2 of article 22 of the GDPR, as only certain decisions that are based on automated decision-making are admissible (Hert, Lazcoz, 2021). These decisions, in principle, are prohibited, unless the decision is based on contractual necessity[32], authorized by EU or Member State's law[33] or there is an explicit consent of the data subject[34].

This was also the position adopted by Article 29 Working Party, later endorsed by the European Data Protection Board[35], where it is stated that "the term right in the provision does not mean that Article paragraph 1 of article 22 applies only when actively invoked by the data subject", as paragraph 1 of article 22 "establishes a general prohibition for decision-making based solely on automated processing[36]".

Recently, the Court of Justice of the European Union ("CJEU") addressed for the first time its first ruling regarding article 22 of the GDPR, on the landmarking case *Schufa Holding (Scoring)*[37]. This was initially referred by the Administrative Court of Wiesbaden, following an appeal made by the data subject who was refused a loan by her bank due to her negative credit score. The negative credit score was produced by SCHUFA, who simply

30. Judgment of Hellenic Data Protection Authority of 19/11/2021. Procedure 51/2021, https://www.dpa.gr/el/enimerwtiko/prakseisArxis.

31. See Rebelo (2023: 287).

32. Subparagraph a) of paragraph 2 of article 22 of the GDPR.

33. Subparagraph b) of paragraph 2 of article 22 of the GDPR.

34. Subparagraph b) of paragraph 2 of article 22 of the GDPR.

35. Article 29 Working Party (2017: 1).

36. Article 29 Working Party (2018: 19).

37. Judgment of 7 December 2023, *Schufa Holding*, C-634/21, EU:C:2023:957.

informed the data subject of her relevant score and provided her a general idea of how the calculations had been made. SCHUFA also argued that the credit score did not constitute an automated decision-making for the purpose of article 22 of the GDPR. The CJEU did not have any doubts and it clarified that the provision "lays down a prohibition in principle" and, as a consequence, its infringement "does not need to be invoked individually by such a person[38]".

We do not anticipate the end of this ongoing debate, as nothing ensures that in the future there will not exist a shift of position by the CJEU. Still, it is safe to assume that, from now on, the question seems pacified. This has a tremendous impact for all the parties. The controllers and processors will have to make carefully assessments before enrolling in automated decision-making and profiling, namely evaluate whether there is (or not) a legal basis under article paragraph 2 of article 22 of the GDPR to justify it, which does not include legitimate interests. For this reason, data subjects will be automatically protected and must be informed accordingly if an automated decision-making is made.

This decision of the CJEU constitutes a landmark in the regulation of data protection towards AI. As we know, automated decision-making systems are the beating heart of many AI systems. From this point of view, it is clear that regulators cannot simply ignore the importance of the GDPR. If the situation falls within the scope of this regulation, article 22 will become the main weapon of data subjects to react towards these decisions.

3.2. Shaping the definition of automated decision-making

For controllers and processors, the only way to avoid the prohibition is by arguing that there is not an automated decision-making, as defined on article 22 of the GDPR. These different elements have also led to some controversy, which implies a careful evaluation of its different vectors. First, there must be a "decision", second, that decision must be "based solely on automated processing, including profiling[39]" and, finally, it has to produce "legal effects concerning the data subject or similarly significantly affect him or her".

We shall start by pointing out that the wording of the provision is misleading[40]. It makes a clear reference to "profiling[41]", but this is only one manifestation of what an automated decision-making can be. While all profiling processes imply an automated decision-making, not all automated decision-making can be considered profiling (Barbosa, Félix, 2021: 75; Kumbar, Roth-Isigkeit (n. 56), 291-292; Costa, 2021: 56).

38. Judgment of 7 December 2023, *Schufa Holding*, C-634/21, EU:C:2023:957, paragraph 52.

39. Recital 71 of the GDPR.

40. Also recognized by Kumbar, Roth-Isigkeit (2021: 289).

41. Paragraph 4 of article 4 of the GDPR defines it as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements".

Let us now enter the analysis of the three elements foreseen on paragraph 1 of article 22 of the GDPR. The concept of "decision" has to be interpreted broadly (Barbosa, Félix, 2021: 74-76). As Lee A. Bygrave outlines, this decision does not need to have a specific form, even though it must be distinct from mere preparatory acts (Bygrave, 2020: 532) that prepare, support or complement the decision-making. As mentioned on Recital 71 of the GDPR, the decision may include a measure. On this matter, the CJEU has also clarified that the concept is capable "of including a number of acts which may affect the data subjects in many ways, since that concept is broad enough[42]" and it concluded that the result of calculating a person's creditworthiness in the form of a probability value concerning that person's ability to meet payment commitments is also included. From what we have seen, it is still essential that there is a minimum degree of complexity, "since otherwise even simple if-then connections would fall under the regulation" (Kumbar, Roth-Isigkeit, 2021, 291). This is not, as a consequence, the most controversial element of the provision.

***

Additionally, and this is the most complex requirement to be interpreted, the decision must be "based solely on automated processing, including profiling". This raises the million-dollar question of how much human intervention is needed to meet the requirements of the provision. Therefore, if a human "examines and weighs other factors when making the final decision" will that be excluded from being considered an automated decision-making (Silveira, 2023: 77)?

Once again, the legislator was ambiguous and the way the article is written arises reasons for doubt[43]. Nevertheless, the wording remains very similar to article 15(1) of the Data Protection Directive. Two paths are drawn on this regard. According to the first position, any human intervention, even if minimal, will not constitute an automated decision-making in accordance to article 22 of the GDPR[44]. This interpretation is anchored on the phrase "solely". The European Commission on its initial proposal intended to use the word "*predominantly*", which did not end up on the final proposal. Therefore, it is argued that, with this word not being adopted, it seems that "the strict reading of 'solely' was intended"(Watcher, Mittelsdat, Floridi, 2017: 92).

This strict interpretation endangers the risk of leading to a diminished protection of data subjects. In 2021, the Court of Amsterdam partially rejected a challenge brought by Uber drivers against automated termination

42. Judgment of 7 December 2023, *Schufa Holding*, C-634/21, EU:C:2023:957, paragraph 46. For an analysis of the concept of decision in regards to the medical system, see Kolfschooten (2024: 1-19).

43. See Lazcoz, Hert (2023: 11-13), and Kolfschooten (2024: 11).

44. Mendoza, Bygrave (2017: 11), advocate that "the fact that a large or even predominant part of the decisional process is automated will not attract the application of Article 22".

of their contracts for fraudulent acts[45]. The Court considered that Uber's contract termination did not constitute an automated decision-making, as the decision to temporarily block access to the platform was taken automatically without human intervention, but this temporary blocking did not have a permanent effect. Uber ended up convincing the Court that this algorithm was a mere tool to aid its specialized team of employees to initiate investigations and adopt the final decision relating to fraud. As a result, it concluded that article 22 of the GDPR could not be applicable.

The second interpretation, which was followed by the Article 29 Working Party and later endorsed by the European Data Protection Board[46], considers that it is necessary to exist a meaningful human intervention, rather than just a "token gesture"[47] to nullify the prohibition[48]. Consequentially, the controller will not be able to fabricate a human involvement as a way to escape this provision (Lazcoz, Hert, 2023: 11; Enarsson, Enqvist, Naarttijärvi, 2022, 133; Kaminski, Urban, 2021: 1978). B. Buchner drew a distinction between formal (in which the human intervention only processes and confirms the decision made) and substantive interventions (2018: 224)[49] (in which, the human intervention is more decisive for the outcome known). This interpretation has the advantage of demonstrating that "some forms of human involvement can be superficial or inadequate" (Green, 2022, 6). As a consequence, it is not necessary the existence of an absolute automated decision without any degree of human intervention (2023: 298). At some point, even if minimal, that will exist.

Accordingly, only a meaningful intervention will be enough to justify the inapplicability of article 22. Nevertheless, what is considered to be a "meaningful intervention"? On this particular point, Article 29 Working Party clarified that it is relevant to evaluate whether the decision has been made by someone who has the authority and competence to change it (and, as a part of the analysis, all the relevant data must be taken into account). In addition, as a part of the DPIA[50], the controller should identify and record the degree of any human involvement in the decision-making process and at what stage this takes place. We do not ignore, as G. Lazcoz and P. de Hert recall, that this expression might lift the "discussion to another level of vagueness" (2023: 12), which reinforces the importance of assessing it on a case-by-case analysis.

On this particular point, Vale and Zanfir-Fortuna have enunciated three situations in which the human intervention shall be considered relevant for the purposes of impeding the application of article 22.º (2022: 29):

45. Judgment of the Court Rechtbank Amsterdam on 11/03/2021. Procedure C/13/692003/HA, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1018.

46. See ARTICLE 29 WORKING PARTY (2017: 21).

47. Expression used by ARTICLE 29 WORKING PARTY (2017: 21).

48. ARTICLE 29 WORKING PARTY (2017: 21) gives as an example someone routinely applying automatically generated profiles to individuals without any actual influence on the result.

49. See also Fidalgo (2021: 224).

50. Article 35 of the GDPR.

a. When specific organizational measures are taken in order to ensure a structured and substantial human involvement throughout the decision process;

b. When specific guidelines and additional elements have to be taken into account before reaching a final decision;

c. When internal procedures which are created demand written assessment to be made by case officers on the basis of an automated assessment[51].

This second line of interpretation, which we consider to be the most coherent to the *ratio* of the GDPR, has been followed by many scholars[52] and it has started to be welcomed amongst different decisions.

The CJEU, on *Schufa Holding*, made a tremendous step forward regarding the scope of article 22. Even though this decision concerns credit scoring, one should bear in mind that it will have a relevant impact in today's economy. Thus, the CJEU defended that paragraph 1 of article 22 of the GDPR has to be interpreted as to meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, "to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person[53]".

It is possible to note that the CJEU did not follow this strict approach, as the SCHUFA score was not regarded as a mere preparatory act for the final decision. This reinforces the protection given by article 22 of the GDPR, but it does not mean that all automated scoring systems will be covered by it. A case-by-case analysis will still have to be conducted in each case. Nevertheless, one should not ignore the importance that this judgment will have in all EU's Member-States.

Very recently, the Supreme Administrative Court of Austria ("VwGH")[54], following the decision of the CJEU, interpreted the provision very broadly. *In casu*, a Public Employment Service in Austria, in order to assess the jobseeker's labor opportunities, used an algorithm to calculate the degree of probability for jobseekers to be employed[55]. The output of the algorithm was used as a starting point for different counsellors to work with jobseekers

51. *Ibid*, 29-31.

52. See, for example, Fidalgo (2021: 224), Buchner (2018: 224), Barbosa, Félix (2021: 74), Bygrave (2020: 533), Costa (2021: 58), Rebelo (2023: 296-299).

53. Judgment of 7 December 2023, *Schufa Holding*, C-634/21, EU:C:2023:957, paragraph 73.

54. Judgment of Verwaltungsgerichtshof of 21/12/2023. Procedure 2021/04/0010-11, https://www.vwgh.gv.at/medien/mitteilungen/Ro_2021040010.pdf?9g4sif

55. The algorithm calculated this probability based on several different factors. As an example of the factors taken into consideration, we can mention age, gender, education, health, career history and care responsibilities.

to evaluate their potential and integrate them on the market. Hence, the algorithm was seen as a supportive measure and was not used for job placement, whose decisions were not binding. As a result, the Austrian Data Protection Authority banned its use due to the lack of legal basis under article paragraph 2 of article 22 of the GDPR, decision which was appealed by the controller. The Federal Administrative Court upheld the controller's appeal, as it considered that article 22 was not applicable to the following case.

Nonetheless, after the appeal of the Austrian Data Protection Authority, the Supreme Administrative Court did not follow this approach, as it argued that the use of this algorithm, which determined the probability of integration into the labor market, had to be regarded as an "automated decision-making", within the meaning of paragraph 1 of article 22 of the GDPR. It demonstrated that the probability value could significantly determine the allocation to the intended customer groups[56], even if the result was exclusively used by a public body to provide jobseekers with targeted employment counseling.

It is not irrelevant knowing what must be the line of interpretation followed when assessing the applicability of paragraph 1 of article 22 of the GDPR. The consequence is very clear. We have come to the conclusion that not any minimal intervention is sufficient to not apply the prohibition. It is, therefore, necessary to consider how the process of the decision is being made and which kind of control there is over the merits of such a decision. Nonetheless, and even if we recognize the importance of the most recent CJEU's jurisprudence, paragraph 1 of article 22 of the GDPR remains the center of uncertainty and a change should be considered when an amendment of the GDPR is made[57].

Controllers, in this new era of AI, might still try to avoid being subjected to the prohibition laid down on the provision, by demonstrating the existence of a decisive human intervention. If that is the case, and considering that many AI systems will rely on the processing of personal data, including profiling, all the other provisions of the GDPR will have to be taken into account. In previous cases, even when of paragraph 1 of article 22 was not applicable, Data Protection Authorities have concluded for the violation of several provisions of the Regulation, especially the ones concerning transparency requirements[58]. There is not a blank check for those situations.

***

56. Judgment of Verwaltungsgerichtshof of 21/12/2023. Procedure 2021/04/0010-11, https://www.vwgh.gv.at/medien/mitteilungen/Ro_2021040010.pdf?9g4sif, paragraph 79.

57. See Camões (2024: 56).

58. The Spanish Data Protection Authority considered that the profiling made by CaixaBank could not be seen as an automated decision-making as employees took the final decision on the best commercial approach in each case and, as a result, paragraph 1 of article 22 of the GDPR could not be applicable. Nevertheless, it concluded that the controller did not fulfill its transparency obligations, under articles 13 and 14 of the GDPR, as it failed to ensure a legal basis for the processing.

Finally, it is necessary that the decision produces legal effects concerning the data subject or similarly significantly affects him or her. It is possible to identify two different scenarios.

A legal effect will require that the decision affects someone's legal rights or duties[59] or it affects its legal status[60]. Additionally, even when there are not legal rights at stake, the data subject can still be affected by a decision, whose effect cannot be seen as trivial (Fidalgo, 2021: 225), rather it must be significant[61]. As S. Barbosa and S. Félix outline "similar effects to the legal ones will be those consequences that although do not create an impact on someone's legal rights, will, either way, have a significant weight in their lives" (2021: 76). Therefore, the decision has to affect the circumstances, behavior, or choices of the individual, have a prolonged impact or, in some cases, lead to discriminatory results. Article 29 Working Party recognized that some decisions may in fact "have a significant effect for certain groups of society, such as minority groups or vulnerable adults[62]".

As a result, if all these requirements are met, the prohibition of paragraph 1 of article 22 of the GDPR will be applicable and controllers will have to demonstrate the existence of a proper legal basis for that processing, under paragraph 2 of article 22 of the GDPR, and also comply with all the other obligations laid down on the Regulation.

4. Reconciling the different requirements of the AI Act in regards to human oversight with the GDPR: do we have the right tools to protect data subject's rights in this digital era?

As we have mentioned before, there are cases where both the GDPR and the AI Act will be applicable. Particularly interesting and relevant is observing some the legal obligations imposed to High-Risk AI Systems[63], in particular the one related to the need to implement human oversight[64]. The

59. See Recital 71 of the GDPR. Article 29 Working Party (2017: 21) gives it as an example the termination of a contract.

60. As an example, it is possible to mention the loss of an entitlement of certain social benefits, as mentioned by Lukas, Váradi (2023: 7). Article 29 Working Party (2017: 21) gives as an example the refusal admission to a country or denial of citizenship.

61. Recital 71 of the GDPR gives as an example the refusal of an online credit application and e-recruiting practices without any human intervention. Article 29 Working Party (2017: 21-22).

62. Article 29 Working Party (2017: 21).

63. Article 6 of the AI Act prescribes that an AI system shall be considered to be high-risk when (i) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonization legislation listed in Annex I, (ii) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonization legislation listed in Annex I or (iii) the AI system is referred on Annex III of the Regulation.

64. High-Risk AI Systems shall establish a risk management system throughout the high risk AI system's lifecycle (article 9 of the AI Act), conduct data governance (article 10 of the AI Act), Draw up technical documentation (article 11 of the AI Act), Design their high risk AI system for record-keeping (article 12 of the AI Act), ensure transparency and provision of information to deployers (article 13 of the AI Act) and

AI Act has a complementary nature in regards to the GDPR[65]. Even though their scope of application is distinct, there are grey areas that require a better clarification.

Paragraph 1 of article 14 of the AI Act requires high-risk AI system to be designed and developed in such a way that they can be effectively overseen by natural persons during the period in which they are in use. This human oversight aims to minimize the risks to health, ensure the safety and respect for fundamental rights[66]. Hence, humans should have the capacity to oversee their functioning, ensure that they are used as intended and that their impacts are addressed over the system's lifecycle[67]. Overall, it aims to ensure that "an AI system does not undermine human autonomy or cause other adverse effects[68]".

There are two different moments where this oversight has to be ensured: before the system is placed on the market or put into service[69] (also known as "development phase" [Lazcoz, Hert, 2023: 6]) - and during the use of the system ("use phase" [Lazcoz, Hert, 2023: 6][70]). As a consequence, the first main difference arises: for the automated decision-making within the GDPR's context it will only be relevant this "second stage of AI use" (Lazcoz, Hert, 2023: 6). Before the system is placed on the market or put into service, it will not be possible to identify any decision in accordance to article 22 of the GDPR. For this reason, it will only matter the second phase: whenever the system is being used.

The human oversight must properly understand the relevant capacities of the high-risk AI system and monitor its operation[71], to remain aware of the possible tendency of automatically relying or over-relying on the output produced[72] and correctly interpret the system's output[73], to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse its output[74] and to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state[75].

---

ensure a proper level of accuracy, robustness, and cybersecurity (article 15 of the AI Act).

65. Paragraph 7 of article 2 of the AI Act.

66. Paragraph 2 of article 14 of the AI Act. See Recital 66 of the AI Act.

67. Recital 73 of the AI Act.

68. European Commission (2020: 21).

69. Subparagraph a) of paragraph 3 of article 14 of the AI Act.

70. See subparagraph b) of paragraph 3 of article 14 of the AI Act.

71. Subparagraph a) of paragraph 4 of article 14 of the AI Act.

72. Subparagraph b) of paragraph 4 of article 14 of the AI Act.

73. Subparagraph c) of paragraph 4 of article 14 of the AI Act.

74. Subparagraph d) of paragraph 4 of article 14 of the AI Act.

75. Subparagraph e) of paragraph 4 of article 14 of the AI Act. Additionally, it is important to outline that "for high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that,

This obligation is applicable to both deployers[76] and providers of these systems.

On its White Paper, the European Commission identified four manifestations (non-exhaustive) of what this human oversight[77] can be, namely:

a) the output of the AI system does not become effective unless it has been previously reviewed and validated by a human[78] (Human in the Loop);

b) the output of the AI system becomes immediately effective, but human intervention is ensured afterwards[79] (Human out of the Loop);

c) monitoring of the AI system while in operation and the ability to intervene in real time and deactivate[80] (Human on the Loop);

d) In the design phase, by imposing operational constraints on the AI system.

In fact, this obligation of human oversight is crucial in bringing the system in or out of the scope of article 22 of the GDPR. As we have seen, the definition of automated decision-making is far from being completed and, due to the uncertainty promoted by its wording and the lack of deeper clarification of the meaning of "meaningful" intervention, it is not very clear how these two approaches will coexist.

By taking into practice some of the obligations laid down on the AI Act, we anticipate the regulation being used as a "shield" or, at least, as an excuse to prevent the applicability foreseen on article 22 of the GDPR.

For example, we shall start by outlining one of the measures foreseen on subparagraph e) of paragraph 4 of article 14 of the AI Act. If the deployer intervenes in the operation of the high-risk AI system and interrupts the system through a "stop" button or a similar procedure that allows the system to come to a halt in a safe state, we will not be able to consider – with the existent legal framework on the GDPR – that the human intervention was a mere formality. On the contrary, as long as the deployer actively intervenes

in addition, no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority" (paragraph 5 of article 14 of the AI Act).

76. See paragraph 2 of article 26 of the AI Act.

77. European Commission (2020: 21).

78. For example, the rejection of an application for social security benefits or grant of a visa. This may also happen in recruitment processes, as the last word will be given to the recruiter.

79. The rejection of an application for a credit loan may be processed by an AI system, but human review must be possible.

80. European Commission (2020: 21) gives as an example the use a stop button or procedure is available in a driverless car when a human determines that car operation is not safe.

and that has an impact on the final decision, the prohibition laid down on article 22 of the GDPR will not be applicable.

Having said that, there is a relevant consequence for the data subjects, whenever the AI Act is applicable for the purposes of high-risk AI system. As it is expected, from the data subject's perspective, in this digital era, it is quite important knowing if a certain situation falls or not within the of paragraph 1 of article 22.

Even when it is not possible to apply the prohibition, the data subject will still be protected by the general principles[81] and rights[82] enshrined on the GDPR.

Nonetheless, paragraph 3 of article 22 of the GDPR has an important impact in regards to the data subject's position. First, it ensures a right to express his or her of point of view.

The exercise of this right will only be adequate as long as the controller takes into consideration the main arguments presented by the data subject, even though the controller is not obliged to do so. It is not clear how it can be effectively fulfilled, as within the context of automated-decision making, this would imply a minimum knowledge of how the system works (Barbosa, Félix, 2021: 85-86; Rebelo, 2023: 349), which is something almost impossible to access on a daily basis. It is yet to be seen a further clarification by the CJEU how this right should be effective.

Secondly, it consecrates a right to contest the decision[83], which is "the backbone" of this provision (Lazcoz, Hert, 2023: 10; Hert, Lazcoz, 2021; Kaminski, Urban, 2021: 1979), as it constitutes a "right of recourse rather than a mere opposing" (Barbosa, Félix, 2021: 86). However, it is not explicit how the data subject can contest and if this grants the possibility for a subsequent decision (if that is the case, shall that decision be made by a human or a machine)? From our point of view, it will be ensured by the controller that the same type of decision, as long as the arguments invoked by the data subject are taken into consideration during that process. Nonetheless, the GDPR is not clear and leaves a wide margin of appreciation to the controllers. The specificities inherent to the exercise of the right to contest the decision should have been detailed by the regulation or, at least, the jurisprudence.

Regarding the right to contest the decision, we believe that the concept of "decision" has to be interpreted broadly, which means that the data subject shall have the possibility to contest decisions, as long as it meets the criterion to be qualified as an "automated decision-making".

In a certain way, due to the lack of attention given to this right, a large margin of appreciation has been given to companies and regulators (Kaminski, Urban, 2021: 1982) and it is uncertain which kind of process should be followed. Nonetheless, from our point of view, an *ex post* human intervention

81. Principle of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability (article 5 of the GDPR).

82. See Chapter III of the GDPR.

83. Also foreseen on paragraph 2 of article 15 of the Data Protection Directive.

will not constitute an independent right, rather it must be seen as requirement to satisfy the right to contest the automated decision-making[84].

An ongoing discussion is related to the so-called "right to explanation", which has raised a tremendous discussion amongst scholars.

The debate started when Goodman and Flaxman defended for the first time that the GDPR consecrated a right to explanation, based on Recital 71 of the GDPR and the wording of paragraph 3 of article 22 of the GDPR (Goodman, Flaxman, 2017: 55). Nonetheless, we do not agree with these arguments. On a first note, recitals do not have binding effects, even though they are relevant for purposes of interpretation. On a second note, it is important to recall that the article 22 does not anticipate any right to explanation. Goodman and Flaxman's position allowed, however, to initiate an interesting debate.

On the contrary, Watcher, Mittelstadt and Floridi argue against the existence of a "right to explanation". The authors consider that articles 13 and 14 of the GDPR cannot be used as evidence of "an ex post right to explanation of specific decisions" as they can only be given once the decision has been adopted. Nevertheless, the authors still consider that, if a right to explanation is, in fact, intended, then it should be "explicitly added to a legally binding article of the GDPR" (2017: 80-97).

Selbst and Powles argue that the reading of subparagraph f) of paragraph 1 of article 13, subparagraph g) of paragraph 1 of article 14 and subparagraph h) of paragraph 1 of article 15 of the GDPR, even if at different stages, allow the data subject to be deeply informed, without having it to expressly defend its existence (Selbst, Powles, 2017: 236).

In our opinion, the right to information of the data subject, as it results from subparagraph f) of paragraph 2 of article 13, subparagraph g) of paragraph 2 of article 14 and subparagraph h) of paragraph 1 of article 15 of the GDPR, is enough to ensure that the needed information is given (Selbst, Powles, 2017: 236; Camões, 2024: 55; Moniz, 2023: 201). The name given (whether "right to explanation" or "right to information") is not the most relevant, as what matters the most is ensuring the protection of the data subject. This seems to have been the position adopted by the CJEU, as the court argued that data subject maintains the right to obtain from the controller, in particular, "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[85]".

From now on, the debate might come to an end. The fact is that the AI Act expressly consecrates "a right to explanation of individual decision-making"[86], which is dependent of two requirements: (i) a person must have been subjected to a decision which is was taken by the deployer on the basis

84. Also adopting this position see Lazcoz, Hert (2023: 10). As both Kaminski and Urban point out "contestability relies on transparency—just as due process requires notice, in addition to an opportunity to be heard" - Kaminski and Urban (2021: 1979).

85. Judgment of 7 December 2023, *Schufa Holding*, C-634/21, EU:C:2023:957, paragraph 56.

86. Article 86 of the AI Act.

of the output from a high-risk AI system listed in Annex III[87] and (ii) that decision must have produced legal effects or significantly affected that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights. This right shall not be applicable whenever is it already provided under EU Law[88].

The right to explanation, as laid down on the AI Act, will be relevant for those situations where both regulations are applicable. For example, the use of AI systems for the recruitment or selection of natural persons and to evaluate candidates, which is considered to be a high-risk AI system. In that case, the jobseeker that was not chosen, might request the deployer an explanation of the result produced. If that is the case, it will not be necessary to invoke any right to explanation under the GDPR. For these specific situations, the debate might end.

Nevertheless, the added value of the provision will be somehow limited (Kelder, 2024), as it only intends to be applicable to high-risk AI systems, due to this specific provision. Therefore, for the remaining situations (for example, generative AI), the data subject will have to invoke the right to explanation under the GDPR, which is not certain, as the CJEU might change its position.

The best way to end the ongoing discussion would be to radically change article 22 of the GDPR, in order to introduce the changes that are necessary to give more certainty for data subjects, controllers and processors. The legislator should, as a result, take a step back and rethink the provision.

That being said, the lack of clarification on what constitutes an *ex ante* meaningful intervention endangers making article 22 of the GDPR a provision without enforcement. By taking into account the "human oversight", as foreseen on article 14 of the AI Act, and even though both scopes are different, it will be very easy for controllers to use it as shield to justify the inexistence of an automated decision-making. We do think that the current state of art needs a better clarification in order to avoid deprotecting rights in the digital era.

5. Conclusion

To sum up, we are left with a final question: will it be possible to reconcile the provisions of the GDPR in regards to automated decision-making in this new AI era? This is one of the most delicate topics of the regulation and, even though the Schufa Holding case was useful to end some doctrinal discussions, it is still not clear how can we conciliate the requirement of "meaningful human intervention". Due to the broadness of measures that can be adopted under the AI Act to ensure the fulfillment of "human oversight", there might exist the risk in the future to use the AI Act as a shield to ensure that a certain decision falls outside the scope of paragraph 1 of article 22 of the GDPR. This endangers the risk of making the provision useless. As we have seen, the jurisprudence of the different Data Protection Authorities is very diverse.

There are two paths: either leave everything as it is and wait for new jurisprudence of the CJEU or change the scenario of automated decision-making within the GDPR. Nonetheless, this does not mean that the GDPR

87. With the exemption of systems listed under point 2 thereof.

88. Paragraph 3 of article 86 of the AI Act. See also Recital 171.

will lose its importance in regards to AI, especially whenever the AI Act is not applicable or, even when it is, the AI system does not meet the criteria to be considered a high-risk AI system. If that is the case, then, article 22 of the GDPR will assume the leading role in protection data subject's rights in this age of AI. Due to the continuous evolution of technology, especially with the development of new models of AI, as long as they process personal data in accordance with the scope of the GDPR, article 22 will have a tremendous importance.

We are left with more doubts than certainties and hopefully, from now on, the legislator will make an effort to fill in the existing gaps.

Bibliography

Article 29 Working Party. Opinion 4/2007 on the concept of Personal Data; 2007. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Article 29 Working Party. Guidelines on Automated Decision-Making and Profiling for the purposes of Regulation 2016/679; 2017. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en

Barbosa S, Félix S. Algorithms and the GDPR: An analysis of article 22. Anuário da Proteção de Dados. 2021; pp. 67-93. Available at: https://protecaodedadosue.cedis.fd.unl.pt/anuario-edicao-2021/

Bygrave, LA. (2020). Article 2.º - Automated Individual Decision-Making including profiling. In: Kuner C et al. (coordinator). The EU General Data Protection Regulation (GDPR) A Commentary. Oxford: Oxford University Press; 2020. pp. 523-542

Buchner B. Art. 22. Automatisierte Entscheidungeni m Einzelfall einshlieBlich Profiling. In: Kühling J, Buchner B. (editors). Datenschutz Grundverordnung/BDSG Kommentar. Munich: C.H. Beck; 2016. pp. 508-520

Calvão, F. IA y el algoritmo discriminatorio: ¿Cómo promover la igualdad?. In Sànchez AR, Cordero PT (coordinators). Desafíos éticos, jurídicos y tecnológicos del avance digital. Spain: Iustel; 2024. pp. 75-88

Camões D. Algorithmic bias in this new era: is the GDPR a feasible tool in addressing this issue?. In: Scialdone M. (editor). My Data is Mine – AI, Data Protection, and a Digital Society. Milano: Giuffrè Francis Lefevbre; 2024. pp. 37-57.

Commission Nationale Informatique & Libertés. Entry into force of the European AI Regulation: the first questions and answers from the CNIL; 2024. Available at: https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil

Cordeiro BM. Dados pessoais: conceito, extensão e limites. Revista de Direito Civil. 2018; Volume III (n.º 2). 297-321

Cordeiro BM. Artigo 2.º (Âmbito de aplicação material). In. Cordeiro BM (editor), Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Coimbra: Almedina: 2021. pp. 66-70

Costa IS. A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. Revista Eletrónica de Direito. 2021; Volume 24 (n.º 1). pp. 34-82. Available at: https://cij.up.pt/pt/red/edicoes-anteriores/2021-nordm-1/

David P, Schwemer SF. Rethinking Decisions under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making. Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace. 2023, available at https://ceur-ws.org/Vol-3423/paper8.pdf

Enarsson T, Enqvist L, Naarttijärvi, M. Approaching the Human in the Loop – legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three contexts. Information & Communications Technology Law. 2022; Volume 31 (n.º 1). 123-153

European Commission. White Paper on Artificial Intelligence - A European approach to excellence and trust; 2020. Available at:

https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Data Protection Supervisor. Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems; 2024. Available at: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en

Fidalgo V. Artigo 22.º (Decisões individuais automatizadas, incluindo definição de perfis). In. Cordeiro BM (editor), Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Coimbra: Almedina: 2021. pp. 220-227

Genderen RV. Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics. European Data Protection Law Review. 2017; Volume 3 (Issue 3). pp. 1-15

Goodman B, Flaxman F. European Union Regulations on Algorithmic Decision Making and a "Right to Explanation". AI Magazine. 2017; Volume 3 (n.º 3). pp. 50-57

Green B. The flaws of policies requiring human oversight of government algorithms. Computer Law & Security Review. 2022; Volume 45. pp. 1-22. Available at: https://www.sciencedirect.com/science/article/pii/S0267364922000292

Gregorio G. Digital Constitutionalism in Europe – Reframing Rights and Powers in the Algorithmic Society. Cambridge: Cambridge, Cambridge University Press; 2022

Gregorio G. The Normative Power of Artificial Intelligence. Católica Global School of Law Working Papers n.º 4/2023; 2023. pp. 1-27. Available at https://catolicalaw.fd.lisboa.ucp.pt/faculty-knowledge

Hert P, Lazcoz G. Radical rewriting of Article 22 GDPR on machine decisions in the AI era. European Law Blog; 2021. Available at: https://www.europeanlawblog.eu/pub/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/release/1

Kaminski ME, Malgier G. Algorithmic impact assessments under the GDPR: producing multi-layered explanations. International Data Privacy Law. 2021; Volume 11 (n.º 2). pp. 125-144

Kaminski ME, Urban JM, The Right to Contest AI. Columbia Law Review. 2021; Volume 121 (n.º 7). pp. 1957-2048

Kelder K. On the relative importance of the AI Act right to explanation. The Digital Constitutionalist – The Future of Constitutionalism. 2024; Available at: https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/

Kesa A, Kerikmäe T. Artificial Intelligence and the GDPR: inevitable nemeses?. Tallinn University of Technology. 2020; Volume 10 (n.º 3). pp. 68-90

Kolfschooten HV. A health-conformant reading of the GDPR's right not to be subject to automated decision-making. Medical Law Review. 2024; Volume 32; Issue 3. pp. 1-19

Kumbar, LK, Roth-Isigkeit D. A criterion-based approach to GDRP's explanation requirements for automated individual decision-making. JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law. 2021. Available at: https://www.jipitec.eu/archive/issues/jipitec-12-4-2021/5403

Lazcoz G, Hert P. Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities. Computer Law & Security Review. 2023; Volume 50. pp. 1-20. Available at: https://www.sciencedirect.com/science/article/pii/S0267364923000432

Lukas A, Váradi S. GDPR-compliant AI-based automated decision-making in the world of work. Computer Law & Security Review. 2023; Volume 50. pp. 1-14. Available at: https://www.sciencedirect.com/science/article/pii/S0267364923000584

Mendoza I, Bygrave LA. The Right not to be Subject to Automated Decisions based on Profiling. University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20. 2017; Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855

Moniz GC. Manual de Introdução à Proteção de Dados Pessoais. Coimbra: Almedina; 2023

Pinheiro AS, Gonçalves CJ. Artigo 22.º. In Pinheiro AS et. al, coordinators. Comentário ao Regulamento Geral de Proteção de Dados. Coimbra: Almedina; 2018. pp. 386- 390

Pollicino O, Gregorio G. Digital Constitutionalism in Europe – Reframing Rights and Powers in the Algorithmic Society. In Micklitz HW et. al, editors. Constitutional Challenges in the Algorithmic Society. Cambridge: Cambridge University Press; 2022. pp. 3-24

Pollicino O, Bassini M, Gregorio G. Internet Law and Protection of Fundamental Rights. Milano: Bocconi University Press; 2022

Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology. 2018; Volume 10 (n.º 1). pp. 40-81

Rebelo DM. Inteligência Artificial e Scoring no Crédito ao Consumo. Coimbra: Almedina; 2023

Rubestein, DS. Acquiring Ethical AI. Florida Law Review. 2021; Volume 73 (n.º 3). pp. 747- 819

Silveira, A. Automated individual decision-making and profiling [on case C-634/21 – SCHUFA (Scoring). EU Law Journal. 2023; Volume 8 (n.º 2). pp. 74-85. Available at: https://revistas.uminho.pt/index.php/unio/article/view/4865/5345

Selbest AD, Powles J. Meaningful information and the right to explanation. International Data Privacy Law. 2017; Volume 7 (n.º 4). pp. 233.242

Tosoni L. The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. International Data Privacy Law. 2021; Volume 11 (n.º 2). pp. 145-162

Vale S, Zanfir-Fortuna B. Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities. Future of Privacy Forum. 2022; Available at: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf

Watcher S, Mittelsdat B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law. 2017; Volume 7 (n.º 2). pp. 76-99

Watcher S, Mittelstadt B. A Right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI. Columbia Business Law Review. 2019; (n.º 2). pp. 496-620

Winau M. Areas of Tension in the Application of AI and Data Protection Law. European Data Protection Law Review. 2023; Volume 2. pp. 123-135

Legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024

Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995

Jurisprudence

Judgment of the Court Rechtbank Amsterdam on 11/03/2021. Procedure C/13/692003/HA, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1018

Judgment of the Hellenic Data Protection Authority of 19/11/2021. Procedure 51/2021, https://www.dpa.gr/el/enimerwtiko/prakseisArxis

Judgment of Verwaltungsgerichtshof of 21/12/2023. Procedure 2021/04/0010-11, https://www.vwgh.gv.at/medien/mitteilungen/Ro_2021040010.pdf?9g4sif.

Judgment of 20 December 2017, *Novak*, C-434/16, EU:C:2017:994

Judgment of 7 December 2023, *Schufa Holding*, C-634/21, EU:C:2023:957