INSIGHT

AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?

Fabienne Ufert*

Abstract: In early 2020, the European Commission published a White Paper on artificial intelligence (AI) regulation, in which it highlighted the need to review the EU's legislative framework with a view to making it fit for the current technological developments. The aim of this *Insight* is to carry out such review from the perspective of fundamental rights. The *Insight* briefly assesses the Commission's concerns surrounding the suitability of the Union's primary legal framework to address the risks posed by AI. More specifically, the analysis is focused on the question concerning how well the GDPR addresses the challenges posed by AI to the fundamental rights of privacy, personal data protection, and non-discrimination – which are the three main intersections between AI and fundamental rights. The perspective adopted in the present study is particularly relevant because the need to regulate AI through the lens of fundamental rights law is still largely underdeveloped. Fundamental rights concerns are mainly triggered when the development and use of AI concern the processing of personal data and thus fall within the scope of application of the GDPR. In this *Insight*, it is argued that the GDPR is well equipped to disruptively challenge actual or potential undesirable uses and applications of AI but some deficiencies are also clearly visible. In particular, in relation to the concept of specific consent, the scope of the data subject's right to information, and on how best to conduct data protection impact assessments when it comes to guaranteeing a trustworthy fundamental rights compliance of the technology.

Keywords: artificial intelligence regulation – artificial intelligence – data protection principles – fundamental rights – GDPR – trustworthy artificial intelligence.

* Student Research Assistant, LLB Graduate in International & European Law, The Hague University of Applied Sciences, fabienne-ufert@t-online.de. The Author wishes to thank Dr. Luca Pantaleo for his valuable assistance and the peer reviewers for their insightful comments. Any mistakes remain those of the Author.

ISSN 2499-8249
doi: 10.15166/2499-8249/394

I. Introduction

I.1. AI and the need for a system of governance

The emergence of Artificial Intelligence (AI) has great potential to enhance social welfare but bears risks at the same time.[1] From a fundamental rights perspective, one can identify biased, discriminatory AI and AI infringements on the rights to privacy and data protection as the main concerns surrounding this technology.[2] Therefore, how best to impose regulations on AI without unnecessarily restricting its development and, at the same time, uphold our society's core values and fundamental rights protection, is an omnipresent question. Seeing that AI is complex, comes in different forms, and intersects with many different areas of law, one specific regulation of AI is most likely not suitable.[3] Instead, a system of AI governance based on the already existing legal framework, composed of specific and general regulations, should be established to address the dynamic nature of AI.[4] The EU's comprehensive legal framework seems to provide the needed prerequisites to establish a system of AI governance, not only within the EU but which can also be influential on the international level. In its White Paper on AI regulation published on 19 February 2020, the Commission agreed on such a system of AI governance.[5] While already pointing out the main intersections between EU law and AI, the Commission states that it considers it necessary to review and complement the legislative framework to make it fit for the current technological developments and to take fully into account the human and ethical considerations of AI.[6] Conducting such a review from a fundamental rights point of view is particularly relevant because the approach of addressing the challenges posed by AI and potentially regulating AI through fundamental rights law is still underdeveloped.[7]

[1] G. Mazzini, *A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law*, in A. De Franceschi, R. Schulze (eds), *Digital Revolutions – New challenges for Law*, Munich: C.H. Beck, 2019, pp. 1, 3-4.

[2] F. Fitsilis, *Imposing Regulations on Advanced Algorithms*, Berlin: Springer, 2019, p. 13; R. Calo, *Peeping HALs: Making Sense of Artificial Intelligence and Privacy*, in *European Journal of Legal Studies*, 2010, p. 171; L. Marin, K. Kraijciková, *Deploying Drones in Policing Southern European Border: Constraints and Challenges for Data Protection and Human Rights*, in A. Zavrsnik (ed.), *Drones and Unmanned Aerial Systems*, Berlin: Springer, 2016, p. 110.

[3] G. Mazzini, *A System of Governance*, cit., p. 4; S. Wrigley, *Taming Artificial Intelligence: "Bots", the GDPR and Regulatory Approaches*, in M. Corrales, M. Fenwick, N. Forgó (eds), *Robotics, AI and the Future of Law*, Berlin: Springer, 2018, p. 187.

[4] G. Mazzini, *A System of Governance*, cit., p. 4.

[5] Communication COM(2020) 65 final of 19 February 2020 from the Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*.

[6] *Ibid*., pp. 10 and 13.

[7] L. McGregor, D. Murray, V. Ng, *International Human Rights Law as a Framework for Algorithmic Accountability*, in *Proceedings of Machine Learning Research*, 2018, p. 311.

This *Insight* conducts parts of this review by briefly analysing the EU's primary legal framework, as well as more comprehensively analysing the General Data Protection Regulation (GDPR) from the perspective of the fundamental rights of privacy, personal data protection, and non-discrimination. The focus is set on reviewing the GDPR because AI is most likely to pose risks to the three identified fundamental rights when processing personal data, hence when the development and/or use of AI falls within the scope of application of the GDPR.[8] Moreover, it is specifically interesting to look at the GDPR in the given context because the GDPR constitutes a great example of a complex but flexible piece of legislation and is thus especially suitable to contribute to a system of AI governance as described above.[9] This is because the GDPR combines (1) general rules, including the provisions that apply equally to processing of personal data by humans and by automated means; (2) specific rules including the provisions that are concerned with processing by automated means; and (3) co-regulatory rules, namely the provisions that require data controllers to analyse and mitigate the risks of the means used for processing on their own, thus giving them the discretion to self-regulate within the bounds of the general protection standards laid down by the GDPR.[10] The *Insight* will conclude that the GDPR is generally well equipped to address the challenges posed by AI to the rights to privacy, personal data protection, and non-discrimination but that more specific provisions solely applicable to AI and its particular characteristics may need to be adopted to safeguard a continuous level of fundamental rights protection.

I.2. Introduction to AI and the risks it poses to fundamental rights

In 2019, the EU's High-Level Expert Group (HLEG) on AI published an updated definition of AI, including its main capabilities and scientific disciplines.[11] According to this definition, AI systems are designed by humans but can come in different forms, such as machine learning, machine reasoning, and robotics. In all its forms but to varying degrees, AI is currently capable of acquiring, processing, and interpreting large amounts of data, making decisions based on the interpreted data, and translating these decisions into action.[12] Based on what AI is capable of, four specific characteristics become visible which, however, do not only come with benefits but may also lead to fundamental rights concerns. First, AI is dependent on data, hence, it has enhanced capacities to col-

[8] Art. 2, para. 1, of 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 personal data.

[9] P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, in *Common Market Law Review*, 2018, p. 4.

[10] S. Wrigley, *Taming Artificial Intelligence*, cit., p. 188.

[11] High-Level Expert Group on Artificial Intelligence (HLEG), *A Definition of AI: Main Capabilities and Disciplines*, ec.europa.eu, p. 6.

[12] *Ibid*., cit., p. 1.

lect and process large amounts of data. This gives AI an increased power of human observation, for example, through biometric identification in public places, thus raising privacy concerns.[13] Secondly, through the connectivity of many AI systems and by analysing large amounts of data and identifying links among them, AI may be used to de-anonymise large data sets although such data sets do not include personal data per se.[14] Thirdly, based on the self-learning ability of AI and, hence, its increasing autonomy, coupled with the enhanced capacity of AI to learn quickly and explore decision paths that humans might not have thought about, AI is able to find patterns of correlation within datasets without necessarily making a statement on causation.[15] Consequently, AI may produce new solutions that may be impossible for humans to grasp by making decisions without the reasons being known, potentially resulting in AI opaqueness. This opaqueness is also known as the 'black-box phenomenon' which drastically reduces the explainability of AI.[16] Fourthly, the training data of AI systems may be biased, leading to AI systems producing discriminatory results.[17]

II. An assessment of the Commission's concerns surrounding the EU's primary legal framework's suitability to address the risks posed by AI to fundamental rights

The EU Treaties provide for a general guarantee of fundamental rights protection.[18] Nonetheless, general principles of EU law have been constituting the principal source of fundamental rights protection in the EU whereby the Charter of Fundamental Rights of the EU (the Charter) now codifies these fundamental rights.[19] Specifically, Arts 7, 8, and 21 lay down the rights to privacy, protection of personal data, and non-discrimination, respectively.[20] The European Commission has expressed concerns regarding the limited scope of application of the EU Charter in the context of the present discussion.[21] According to Art. 51 of the Charter and the case law of the Court of Justice, the Charter and gen-

[13] Communication COM(2020) 64 final of 19 February 2020 from the Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, p. 2; *White Paper on Artificial Intelligence*, cit., pp. 21-22.

[14] *White Paper on Artificial Intelligence*, cit., p.11; COM(2020) 64, cit., p. 2.

[15] HLEG, *A Definition of AI*, cit., p. 1.

[16] *Ibid*., p. 5; COM(2020) 64, cit., p. 2.

[17] HLEG, *A Definition of AI*, cit., p. 5.

[18] Art. 2 TEU.

[19] The CJEU accepted fundamental rights as general principles of EU law between the *Solange I* and *Solange II* judgments by the German Constitutional Court. See Court of Justice, judgment of 17 December 1970, case 11-70, *Internationale Handelsgesellschaft*, para. 4.

[20] Arts 7, 8 and 21 of the Charter.

[21] European Commission, *Structure for the White Paper on artificial intelligence – a European approach*, Leaked White Paper on AI, euractiv.com, p. 11.

eral principles of EU law apply to any action falling within the scope of EU law.[22] Consequently, certain Member States' actions involving the development and/or use of AI systems may not fall within the Charter's field of application and may, thus, potentially lead to a compromised fundamental rights protection. For example, the use of AI systems in the industry or the health sector is only partially or not covered at all by the Charter's scope of application because these fields fall primarily within the exclusive competences of the Member States.[23] Nevertheless, the EU often takes on an active supportive role to protect fundamental rights by adopting guidelines, even in areas that fall outside its main competences. For example, in the health sector, the Commission has adopted guidelines for Member States on the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) app, designed to help tackle the Covid-19 crisis by tracing infection chains, even across borders.[24] The app is largely based on advanced algorithms and, hence, touches upon privacy and data protection concerns of interest by the Union.

Another concern that was raised by the Commission was the lack of horizontal direct effect of the Charter.[25] However, it must be noted that the Court has practically acknowledged the direct horizontal application of the Charter in specific situations, namely when EU secondary law gives expression to a general principle of EU law, such as the principles of privacy and protection of personal data and non-discrimination.[26] Hence, the use of AI systems must be in conformity with these principles, even in horizontal situations falling within the scope of EU law. For example, the observance of the principle of non-discrimination in situations covered by Directive 2000/78/EC on equal treatment in employment and occupation is particularly important when AI systems are used for recruitment purposes in employment matters, amongst others.[27]

In conclusion, the Commission's concerns seem rather unfounded. Nonetheless, the Charter does not apply in situations falling outside the scope of EU law, even in situations where the Court has acknowledged the so-called horizontal direct effect of the Charter. While this is logical, it may lead to a fragmentation of the internal market when

[22] Art. 51, para. 1, of the Charter; for general principles of EU law, see Court of Justice, judgment of 18 December 1997, case C-309/96, *Annibaldi*, paras 13-14; for the Charter, see Court of Justice: judgment of 26 February 2013, case C-617/10, *Akerberg Fransson* [GC], para. 44; judgment of 19 November 2019, joined cases C-609/17 and C-610/17, *TSN and AKT*, paras 43 and 53.

[23] Art. 6, let. a) and b), TFEU.

[24] eHealth Network, *Mobile applications to support contact tracing in the EU's fight against COVID-19 – Common EU Toolbox for Member States*, ec.europa.eu, p. 10.

[25] Structure for the White Paper on artificial intelligence, cit., p. 11.

[26] Court of Justice, judgment of 19 January 2010, case C-555/07, *Kücükdeveci*, para 27. The rights to privacy and protection of personal data, and the right to non-discrimination, constitute general principles of EU law, see Court of Justice: judgment of 17 July 2014, joined cases C-141/12 and C-372/12, *YS and Others*, para 54; judgment of 22 November 2005, case C-144/04, *Mangold*, para 75, respectively.

[27] For the use of AI systems for recruitment processes, see White Paper on Artificial Intelligence, cit., p. 18; S. HÄNOLD, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, in M. CORRALES, M. FENWICK, N. FORGÓ (eds), *Robotics, AI and the Future of Law*, Berlin: Springer, 2018, p. 128.

it comes to developing and using AI systems by various actors, including the compliance of such AI systems with fundamental rights.[28] Moreover, there may be situations in which it is difficult to rely on the limited horizontal direct effect of the Charter – a gap that may be filled by pieces of EU secondary legislation like the GDPR.

III. An analysis of how well the GDPR addresses the challenges posed by AI to the fundamental rights of privacy, personal data protection, and non-discrimination

The GDPR is, amongst others, specifically intended to apply to partly or fully automatic AI systems that process personal data forming part or intended to form part of a filing system.[29] At the same time, the use of AI systems is limited under the GDPR. For example, while the GDPR applies to the processing of personal data by wholly automated means, Art. 22, para. 1, prohibits the use of fully autonomous AI systems for the processing of personal data which produces legal effects for individuals.[30] Hence, the GDPR limits the development and use of AI to systems that still function with some sort of meaningful human oversight.[31] Additionally, also functioning as one exception to the prohibition laid down in Art. 22, para. 1, the processing of personal data can only take place based on the specific consent of the data subject.[32] The concept of specific consent entails informed consent, meaning that the data subject must not only be informed that her personal data is being processed but also about how and for what purposes the processing takes place.[33] While, in theory, the requirement of consent should provide for sufficient safeguards against fundamental rights violations by AI systems processing personal data, it is difficult to obtain informed consent when AI systems make unpredictable decisions.[34] Moreover, the means of obtaining the specific consent of the data subject, such as "I have read and agree to the Terms", is one of the biggest lies on the internet that poses the risk of rendering the protection offered by the concept of specific consent inefficient.[35] To avoid this, it can be as-

[28] White Paper on Artificial Intelligence, cit., p. 10.

[29] Art. 2, para. 1, of Regulation 2016/679, cit.

[30] *Ibid.*, Art. 22, para. 1.

[31] "Meaningful human oversight" is the same as "meaningful human involvement". To qualify as such, the oversight of a decision made by AI must be meaningful, rather than a token gesture. This means that it should be carried out by someone who has the authority and competence to change the decision and, as part of the analysis of the decision, this person should consider all the relevant data. See Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, p. 21.

[32] Art. 6, para. 1, let. a), Art. 9, para. 2, let. a), Art. 22, para. 2, let. c), of Regulation 2016/679, cit.

[33] Court of Justice, judgment of 24 September 2019, case C-136/17, *GC and Others v. CNIL*, para. 62.

[34] S. Wrigley, *Taming Artificial Intelligence*, cit., p. 192; S. Hänold, *Profiling and Automated Decision-Making*, cit., pp. 137 and 147.

[35] S. Wrigley, *Taming Artificial Intelligence*, cit., p. 196; S. Hänold, *Profiling and Automated Decision-Making*, cit., p. 137.

sumed that the use of fully, as well as partly automated AI systems, is further limited by the principle of controller responsibility under the GDPR.[36] For example, in *Google Spain*, the CJEU found that a search engine operator is a controller within the meaning of Art. 4, para. 7, GDPR when she processes personal data.[37] This is when the activity of the search engine consists of finding information, indexing it automatically, storing it temporarily, and making it available to internet users, when that information consists of personal data.[38] If this is the case, the controller has a responsibility to, under specific circumstances, remove searches based on a person's name from the list of results.[39] Although certain of these processing procedures by a search engine may be done by AI systems, it is the search engine operator who has the ultimate responsibility, thus limiting the use of AI systems in such circumstances. Moreover, in *GC and Others v. CNIL*, the Court held that it is the responsibility of a search engine operator, when receiving a de-referencing request, to balance the right to personal data protection against other rights which may be affected by the de-referencing, for example, the right to freedom of information.[40] Hence again, the use of AI systems for the operation of search engines is limited by the operator's responsibility to oversee and guarantee the necessary fundamental rights protection. In conclusion, this means that the full potential of AI can never be used in situations falling under the GDPR. Considering this in the light of fundamental rights, the development and use of AI systems are generally limited by the concepts of specific consent and controller responsibility to safeguard the protection of the rights of the data subjects.

Moreover, one should look at the issues arising from the typical characteristics of AI systems, and which trigger fundamental rights concerns, and how the GDPR specifically responds to these issues. To recall, in light of the fundamental rights of privacy, personal data protection, and non-discrimination, the main concerns surrounding AI constitute its increased capacities of human observation, the potential to de-anonymise large data sets, opaque decision-making, and the production of discriminatory results. The concern of increased human observation through AI is specifically met by the prohibition of processing special categories of personal data, such as biometric data.[41] When it comes to the potential de-anonymisation of data sets by AI, the GDPR attempts to regulate this concern by, subject to a few exceptions, the same prohibition of the processing of special categories of personal data, including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data, health data, and data concerning a natural person's sex life or sexual orientation. Hence, once an AI system de-anonymised such

[36] Arts 5, para. 2, and 82, para. 2, of Regulation 2016/679, cit.
[37] Court of Justice, judgment of 13 May 2014, case C-131/12, *Google Spain* [GC], para. 41.
[38] *Ibid*., para. 41.
[39] *Ibid*., para. 88.
[40] *GC and Others v. CNIL*, cit., paras 57, 66, 68.
[41] Art. 9, para. 1, of Regulation 2016/679, cit.

data leading back to a natural person, the processing would probably need to be aborted. In light thereof, it has been argued that the GDPR provides data subjects with control over how their personal data is collected and processed but only very little control over how the data is evaluated and, hence, used to draw inferences about the data subjects.[42] In several cases, the Court held that, if a data subject wishes to challenge evaluations of her personal data, recourse must be sought through sectoral laws applicable to the specific situations in question and not through the existing data protection laws.[43] This leads one to the conclusion that the Court does not regard inferences from personal data as personal data itself and thus, such inferences do not fall within the scope of the EU's legislation on personal data protection. In *YS and Others*, the Court confirmed that the analysis of personal data cannot in itself be so classified.[44] On the other hand, in *Nowak*, the Court acknowledged a broader concept of personal data, including not only factual information but also opinions and assessments.[45] However, such opinions and assessments, which can be classified as inferences drawn from personal data, do not generally constitute personal data but only in certain circumstances, evaluated based on a case-by-case assessment.[46] Hence, the Court still followed its previous approach by granting only limited rights to data subjects over assessments of their personal data. The limited rights of data subjects over inferences drawn from their personal data become problematic when it comes to Big Data analytics through AI systems and their capabilities of de-anonymising datasets that seem 'not personal' *prima facie*, especially because such inferences are often used to make important decisions regarding the data subject in question.[47]

As regards the opacity in AI decision-making, the GDPR requires the observance of the principles of transparency and explainability, including the data subject's rights to information and access to personal data.[48] To uphold these principles, this also includes *ex ante* measures within the development phase of AI systems, such as conducting data protection impact assessments (DPIA) and implementing appropriate technical and organisational measures to help implement the data protection principles, also called data protection by design.[49] This means that developers of AI systems have a duty to build in safeguards that provide for a guarantee to uphold the data protection principles in the first place. In light thereof, three issues arise. First, the concept of personal data in Art. 4, para.

[42] S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI*, in Columbia Business Law Review, 2019, pp. 6-7.

[43] Court of Justice: judgment of 29 June 2010, case C-28/08, *Commission v. Bavarian Lager*, paras 49-50; judgment of 20 December 2017, case C-434/16, *Nowak*, paras 54-55; *YS and Others*, cit., paras 45-47.

[44] *YS and Others*, cit., para. 48.

[45] *Nowak*, cit., paras 34-35.

[46] *Ibid*., para. 53.

[47] S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences*, cit., p. 7.

[48] Art. 5, para. 1, let. a), Art. 12, para. 1, Art. 15, para. 1, and Art. 20 of Regulation 2016/679, cit.

[49] *Ibid.*, Arts 25, para. 1, and 35.

1, of the GDPR is very broad and has been further expanded by the Court in cases like *YS and Others*, *Nowak*, and *Breyer*.[50] Hence, it is not exhaustively defined what personal data is which may make it difficult to determine the bounds of AI use for data processing purposes.[51] This is problematic because AI systems cannot necessarily be simply aborted if they become independent, hence, the bounds of AI use should be determined in the development phase already.[52] On the other hand, a broad concept of personal data guarantees to cover nearly all eventualities and thus reflects a technological reality.[53] The very fact that a piece of information has been created or merely distributed by an individual may provide some clues about who that individual may be and AI is able to detect such correlations better than humans.[54] Secondly, seeing that the concept of personal data is not exhaustively defined, the scope of the right to information is also disputed.[55] For example, and es previously mentioned, it is disputed whether inferences drawn from personal data constitute personal data themselves and should thus be included in the data subject's rights to information and access to personal data. Additionally, due to AI complexity, there exists the risk that controllers use that complexity and the autonomy of AI as an excuse to circumvent their information and access to personal data obligations towards the data subject.[56] Although it is arguable that, from a fundamental rights perspective, AI systems that cannot meet the data protection principles and uphold the rights of the data subject should not be developed in the first place, this would strongly limit the use of AI for personal data processing purposes.[57] Consequently, it would be useful to better specify the scope of the right to information in relation to the processing of personal data by AI systems to guarantee GDPR compliant AI use. Thirdly, Art. 25 (data protection by design), complemented by Art. 35 (data protection impact assessment) impose a duty on controllers to implement appropriate technical and organisational measures to ensure compliance with the GDPR both when planning and performing the processing of personal data and, thus, encourages controllers to think ethically *ex ante*.[58] However, within this approach, there exists the concern that DPIAs may result in a 'rubber-stamping' procedure.[59] This means that, again, the complexity of AI could be used as an excuse not to actually assess the results produced by AI systems in light of their compliance with the

[50] *Ibid.*, Art. 4, paras 1-2.; *YS and Others*, cit., para. 48; *Nowak*, cit., paras 46, 49 and 62; Court of Justice, judgment of 19 October 2016, case C-582/14, *Breyer*, para. 49.

[51] S. WRIGLEY, *Taming Artificial Intelligence*, cit., pp. 191-192.

[52] G. SARTOR, *Liabilities of Internet Users and Providers*, in M. CREMONA (ed.), *New Technologies and EU Law*, Oxford: Oxford University Press, 2017, p. 176.

[53] *Ibid.*

[54] *Ibid.*

[55] S. HÄNOLD, *Profiling and Automated Decision-Making*, cit., p. 143.

[56] *Ibid*., p. 143.

[57] S. WRIGLEY, *Taming Artificial Intelligence*, cit., pp. 192-193.

[58] Arts 25 and 35 of Regulation 2016/679, cit.

[59] S. WRIGLEY, *Taming Artificial Intelligence*, cit., pp. 196 and 200.

GDPR but merely let these results be approved by a human to be able to say that there were human oversight and risk assessment.[60]

Lastly, regarding AI discrimination, the GDPR's prohibition of the processing of special categories of personal data – meaning data that also constitute potential grounds for discrimination – by solely automated means offers a concrete protection against AI discrimination.[61] Unfortunately, the special categories of personal data laid down in Art. 9, para. 1, of the GPDR do not include the categories of colour, language, membership of a national minority, property, and birth which are, however, recognised as grounds of discrimination in Art. 21, para. 1, of the Charter.[62] This constitutes a potential gap in the prevention of discriminatory results through personal data processing, both by AI systems and conventional means. Moreover, Art. 22, para. 1, GDPR, further underlined by Art. 35, para. 3, prohibits profiling by fully automated means.[63] Profiling is a form of processing carried out on personal data to evaluate personal aspects about a natural person and, as the name says, create profiles.[64] This process places people in categories based on their personal traits and is thus likely to lead to discrimination.[65] More specifically, data subjects are likely to be objectified because AI systems evaluate individuals by the probability of a group based on correlation and statistical models and thus do not regard individuals in light of their own rights.[66] The prohibition in Art. 22, para. 1, GDPR provides for guarantees against such discrimination. However, the data subject's specific consent constitutes an exception to the prohibition whereby the same issues surrounding specific consent as explained above may arise, thus rendering the protection granted by Art. 22, para. 1, of the data subject's rights inefficient.[67]

IV. Conclusion

First and foremost, this *Insight* has demonstrated that within the primary legal framework on the rights to privacy, personal data protection, and non-discrimination, the limited scope of application of the Charter may create difficulties when it comes to a comprehensive fundamental rights protection against the challenges posed by AI. However,

[60] *Ibid.*

[61] Art. 9, para. 1, of Regulation 2016/679, cit.

[62] Art. 21, para. 1, of the Charter.

[63] Arts 22, para. 1, and 35, para. 3, let. a), of Regulation 2016/679, cit.; On how the GDPR may further contribute to fair and anti-discriminatory AI, see P. Hacker, *Teaching Fairness to Artificial Intelligence*, cit., especially pp. 24-34.

[64] Art. 4, para. 4, of Regulation 2016/679, cit.; Article 29 Data Protection Working Party, *Guidelines*, cit., pp. 5 and 7.

[65] Art. 29 Data Protection Working Party, *Guidelines*, cit., p. 6.

[66] S. Hänold, *Profiling and Automated Decision-Making*, cit., p. 130.

[67] Art. 22, para. 2, let. c), of Regulation 2016/679, cit.; S. Wrigley, *Taming Artificial Intelligence*, cit., p. 196; S. Hänold, *Profiling and Automated Decision-Making*, cit., p. 137.

where the scope of application of the Charter reaches its limits, pieces of secondary legal instruments with direct effect like the GDPR are very valuable. Due to its comprehensive and flexible nature, the GDPR is especially well suited to contribute to a system of AI governance in the EU and even be influential on the international plane. This is because the EU's comprehensive legal instruments on fundamental rights protection, such as the GDPR, highlight the EU's distinct vision to perpetuate the values of respect for human dignity, pluralism, non-discrimination, and protection of privacy anywhere. For example, cases like *Schrems* and opinion 1/15 show that the EU only allows the transfer of personal data to third countries if these countries can provide for equivalent personal data protection standards as laid down in the GDPR, especially if the processing of this data is carried out by automated means.[68]

Now, overall, the GDPR has certainly the potential to disruptively challenge actual or potential undesirable uses and applications of AI systems because the instrument's different provisions address all challenges that AI poses to privacy, personal data protection, and the prohibition of discrimination.[69] However, the question is how well the GDPR addresses these challenges posed by AI? First, any case of personal data processing must usually be based on the specific consent of the data subject but this requirement of often being disrespected by a simple click on the "yes" box under several pages of Terms and Conditions and/or the reduced explainability of certain AI systems. Secondly, the concept of personal data is not exhaustively defined and thus the scope of the right to information under the GDPR is disputed. It is especially unclear if inferences drawn from personal data – something that AI is particularly good at – form part of the concept. Thirdly, AI complexity and its reduced explainability pose the risk of triggering so-called 'rubber-stamping' procedures whereby controllers circumvent the GDPR guarantees against unlawful AI use for the processing of personal data when conducting DPIAs. So far, the EU's definition of AI limits AI systems to be "designed by humans" and the GDPR reflects this aspect by requiring meaningful human oversight for the use of automated means.[70] However, AI has already developed and will continue to do so beyond how it is currently defined by the EU and, in this further developed form, will become more and more part of our daily lives. Consequently, the EU will need to fill gaps like the issues surrounding the concept of specific consent and 'rubber-stamping' DPIAs by means of more specific provisions applicable to AI and its particular characteristics that are different from human action. Only like this, the development and use of AI can be fully compliant with fundamental rights which is crucial for the creation of the necessary trust in this technology.

[68] Court of Justice: judgment of 6 October 2015, case C-362/14, *Schrems*, para. 73; opinion 1/15 of 26 July 2017, paras 168-174.

[69] G. MAZZINI, *A System of Governance*, cit., p. 34.

[70] HLEG, *A Definition of AI*, cit., p. 6.