The Normative Potential of the European Rule on Automated Decisions: A New Reading for Art. 22 GDPR

*Christian Djeffal**

* The author is Tenure Track Assistant Professor for Law, Science and Technology at Munich Center for Technology in Society and TUM School of Governance at Technical University Munich. The author thanks Mr. *Nicolas Fischer* for his help in preparing this article.

Abstract

This article looks into the normative potential of the rule on automated decisions in the European Union's (EU's) General Data Protection Regulation (GDPR). It explains the regulative approach taken in Art. 22 GDPR and reveals its nature as a law by design obligation. To comply with Art. 22 GDPR, it is not enough to abide by a strict set of rules. The technological and socio-technical design of each automated decision-making system (ADMS) has to be performed in a way that is in accordance with the data subject's rights and freedoms and legitimate interests. Art. 22 GDPR, therefore, requires a full assessment of the positive and negative impacts of the ADMS and the measures to mitigate them. The article also looks into the

legislative history of Art. 22 GDPR and shows how emerging technologies were addressed over the years and what the state of the art is in Member States of Convention 108. Finally, it inquires into current trends of the regulation of ADMS in the context of European Union law.

I. Introduction

Artificial intelligence (AI) is the source of many hopes and fears, challenges and opportunities.[1] There have been many discussions about the role of regulation in AI development and its use in society. This contribution looks at Art. 22 of the EU's General Data Protection Regulation, a European norm concerning automated decision-making.[2] In the face of many calls to regulate artificial intelligence, this contribution probes the normative potential of Art. 22 GDPR in the face of new possibilities of AI systems. In order to do that, this article will map out the history of this provision, current quarrels concerning its interpretation and its potential futures. Most importantly, I will argue that Art. 22 GDPR is a law-by-design clause that forces to include legal rights, freedoms, and interests into the design of technology. This interpretation helps to meet current challenges of ADMS in the face of new possibilities afforded by artificial intelligence.

This is warranted since machine learning technologies are constantly improving their capacity to solve tasks, especially through deep neural networks.[3] In some instances, the general public has reacted with amazement and awe when AI systems seemingly performed the impossible by doing tasks thought to be the exclusive purview of human intelligence. This was the case when AI systems beat humans in games like Go or Poker or even won debating challenges. In other cases, AI systems became part of our dai-

[1] IEEE, Ethically aligned design, Version 2, 2018, <https://ethicsinaction.ieee.org>; Future of Humanity Institute/University of Oxford/Centre for the Study of Existential Risk/University of Cambridge/Centre for a new American Security: Electronic Frontier Foundation/OpenAI, The Malicious Use of Artificial Intelligence, Forecasting, Prevention, and Mitigation, 2018, <https://maliciousaireport.com>.

[2] For the text of this norm, see Appendix VI. 3. d).

[3] Machine learning is one subset of AI technologies. AI is here conceived to be a general research question about systems that can deal with complex problems in an independent manner. For that definition see *K. Mainzer,* Künstliche Intelligenz – Wann übernehmen die Maschinen?, 2019, 3; *C. Djeffal,* Artificial Intelligence and Public Governance, Normative Guidelines for Artificial Intelligence in Government and Public Administration, in: T. Wischmeyer/T. Rademacher (eds.), Regulating Artificial Intelligence, 2020, 277 (278). Introductions can be found in *J. Stuart/J. Russell/P. Norvig/E. Davis,* Artificial Intelligence, A Modern Approach, 2016.; *I. Goodfellow/Y. Bengio/A. Courville,* Deep Learning, 2016.

ly infrastructure without anybody really noticing. Take, for example, intelligent traffic systems that decide to implement overtaking bans or speed limits in an automated fashion. These are implemented all over the world and generally accepted. One major challenge in assessing AI is the fact that the term denotes a whole set of technologies[4] and that those technologies have a general-purpose nature. Like in the case of the printing press or the steam engine, the assessment of the technology depends on its use. Therefore, it is hard to conceive of AI as entirely good or bad. It depends on the context in which AI is assessed. This seems obvious on the face of it but becomes crystal clear in the case of AI discussions at the United Nations (UN). Metaphorically, the way in which AI is discussed in the UN context depends on the time of year you visit Geneva. In spring, the International Telecommunications Union (ITU) hosts the "AI for good" summit. Several stakeholders discuss how to use AI in order to meet the sustainable development goals and share ideas and experiences. In autumn, a Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapon systems (LAWS) meets in order to discuss this highly sensitive issue under the umbrella of the Conference of the High Contracting Parties to the Convention on Certain Conventional Weapons (CCW). Apart from these outliers, AI-based systems taking real-life decisions, so-called automated decision-making systems, are used in many different areas of society such as tax administration, consumer pricing or intelligent traffic systems. These increased capabilities of ADMSs and the challenges they pose have provoked a lively discussion on how to govern and regulate AI in general and ADMSs in particular.[5]

In the face of regulatory challenges posed by emergent technologies, there is commonly an almost instantaneous reaction to call for *new* regulation or, on the flipside, opposition to such regulation. These calls are made with an air of originality and innovation, resting either on regulatory innovation or on the innovative potential of emergent technologies. However, the more painstaking and sometimes painful option is to inquire deeply into the *acquis* of the law currently in application to understand its normative potential *vis-à-vis* the new aspects of the emergent technology. This contribution takes the latter road and aims to discover the normative potential of Art. 22 GDPR by looking into its past, present, and into its possible fu-

[4] *U. Gasser/V. A. F. Almeida,* A Layered Model for AI Governance, IEEE Internet Computing 21 (2017), 58 (58).

[5] To mention only a few examples: *U. Gasser/R. Budish/A. Ashar,* Module on Setting the Stage for AI Governance, Interfaces, Infrastructures, and Institutions for Policymakers and Regulators, in: Artificial Intelligence (AI) for Development Series 2018; *T. Wischmeyer/T. Rademacher* (note 3).

tures. As other norms, legal norms have the capacity to alter the course of things and to bring about possibilities that are different from our *status quo*.[6] Yet, the law is also dependent on and intertwined with the realities it is addressing. Therefore, digital transformation is also shaping the law.[7] In the context of a new digital constellation,[8] I will look into Art. 22 GDPR and try to understand what the known and unknown potentials of this rule might be. While I look into current discussions and future trends, I will also address the legislative history of the provision.

II. Legislative History: A Multilevel Legislative Conversation

One way to understand the normative potential of Art. 22 GDPR is to look back at the legislative history leading up to the creation of this norm. It is an apt example of mirroring emergent technologies with accompanying regulation. We are used to that regulation of technology looking back than rather addressing the past and being slower than technological progress. However, the story of the original idea leading up to Art. 22 GDPR provides us with a forward-looking rule in French law that addressed technologies of the future. The evolution of the regulation of automated decisions is interesting in that it gives evidence of a "legislative conversation" across different levels, such as international law, European law, and national law. Those developments are interrelated and can be read as one continuous evolution.[9] Yet, Art. 22 GDPR also reveals its nature specifically when focusing on how the regulation of an emerging technology evolves and how it takes different steps in the progressive development and adoption of the technology.

The idea to regulate automated decisions was exceptional when first laid out in the French legal order in 1978. However, it proliferated to all member states via European Union law through Directive 95/46/EC and

[6] A deep reflection of these topics can be found in *C. Möllers*, Die Möglichkeit der Normen, Über eine Praxis jenseits von Moralität und Kausalität, 2015.

[7] *M. Hildebrandt,* Legal and Technological Normativity: More (and Less) than Twin Sisters , Techné: Research in Philosophy and Technology 12 (2008), 169.

[8] *I. Pernice,* Global Cybersecurity Governance, A Constitutionalist Analysis, in: Global Constitutionalism 7 (2018), 112 (112).

[9] *P. Häberle,* Textstufen als Entwicklungswege des Verfassungsstaates, Arbeitsthesen zur Verfassungslehre als juristischer Text- und Kulturwissenschaft, in: J. Jekewitz/K. H. Klein/J. D. Kühne/H. Petersmann/R. Wolfrum (Hrsg.), Des Menschen Recht zwischen Freiheit und Verantwortung, Festschrift für Karl Josef Partsch, 1989, 555.

Art. 22 GDPR. Finally, the member states of the Council of Europe's Convention 108 inserted the right of a person

> "not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration"

in Art. 9 Sec. 1 Subsec. a.[10]

Including a rule on automated decisions in data protection laws was far from self-evident in the beginning. Early laws like the Data Protection Act of Hesse (Germany) or the German Data Protection Act did not touch upon this topic at all. Yet, it came up in the discussions leading up to Art. 2 of the French Data Protection Act. A draft of the government's bill contained a prohibition of completely automated decisions in the contexts of courts and public administrations.[11] In the legislative process, the application of this prohibition was substantially widened and applied to private actors, prohibiting fully automated decisions for private actors and public administrations.[12] In the case of the judiciary, even decision support systems were outlawed. The background to the French data protection legislation was a political scandal based on a comprehensive government database called SAFARI.[13] After a news report had revealed that the French government sought to collect all data concerning citizens that it has held by a unique identifier, discussions ultimately led to a law aimed at safeguarding citizens' rights in the face of new computational capabilities. Looking for the normative potential of Art. 22 GDPR, it is important to notice the initial reasons for this prohibition. The respective parliamentary report mentions several interesting aspects:[14] First, the French legislators looked at developments in other jurisdictions, particularly to "crime coefficients" in the United States and reacted to them. While there was a fear concerning the database, the

---

[10] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Council of Europe, CM/Inf(2018)15-final 18.5.2018.

[11] Art. 2 Draft Law No. 2516 of 9.8.1976 on Information Technology and Civil Liberties, see Appendix VI. 1. a).

[12] Art. 2 Act No. 78-17 on Information Technology, Data Files and Civil Liberties, Journal Officiel de la Republique Française 1978, 227, see Appendix VI. 1. b).

[13] Système automatisé pour les fichiers administratifs et le répertoire des individus. For a summary of the development see *D. H. Flaherty,* Protecting Privacy in Surveillance Societies, The Federal Republic of Germany, Sweden, France, Canada, and the United States, 1989, 166 et seq.; *A. Vitalis,* France, in: J. B. Rule/G. Greenleaf (eds.), Global Privacy Protection, 2008, 107 (107).

[14] *J. Thyraud,* Rapport fait nom de la Commission de Lois constitutionnelles, de Législation, du Suffrage universel, du Réglement et d'Administration générale sur le project de loi relatif à l'informatique et aux libertés, 1977, 22, <https://www.senat.fr>.

fear of automated decisions was rather situated in a future scenario. This is remarkable since the current debates about the governance and regulation of algorithms have been centring on the prediction of recidivism before United States (US) Courts, at least initially.[15] The French legislators saw a risk that decisions would lose their "humane character". Yet, they still acknowledged that human decisions might be "fallible".[16] They were concerned about a general "flight from responsibility in the face of the computer", especially in cases in which computers take decisions in which the law has to be interpreted.[17] The *travaux* show a great sensitivity for many of the *topoi* that are still relevant today. However, the respective systems appear more like a distant scenario as compared to specific technical systems in need of regulation. Convention 108 in the Council of Europe[18] – being the first international treaty on data protection – did not touch upon the subject of automated decisions, and only very few states covered this issue in their own data protection laws.[19]

This changed substantively with Directive 95/46/EC, which set out a rule on automated decisions that member states had to transfer into their respective legal orders. Because of Directive 95/46/EC, every member state of the European Union adopted a rule on automated decisions. The links between the French law and Directive 95/46/EC are obvious when looking at the Commission's second draft.[20] It was included in a provision detailing rights of the data subjects. Like the French law, the European Commission initially suggested prohibiting automated decisions generally – without qualifications whatsoever. In the course of the legislative proceedings, the European Parliament[21] substantially changed the draft, as did the European Council.[22] The proposal of the European Parliament shifted the nature of the rule. It added exceptions to the right not to be subject to an automated decision.

---

15 *A. Chouldechova,* Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments, in: Big Data, 2017, 153.; *J. M. Eaglin,* Constructing Recidivism Risk, in: Emory L. J. 67 (2017), 59.

16 *J. Thyraud* (note 14), 22.

17 *J. Thyraud* (note 14), 22.

18 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 18, 28.1.1981, entry into force 1.10.1985.

19 See *U. Brühann,* Art. 15 Directive 95/46/EC, in: E. Grabitz/M. Hilf (Hrsg.), Das Recht der Europäischen Union, 2009.

20 Art. 14 [No. 2] COM(90) 314 final. See Appendix VI. 2. a).

21 Amendment No. 46 Opinion of the European Parliament 0314 - C3-0323/90 on the Proposal for a Directive I COM(90), O.J. 1992,C 94/173, see Appendix VI. 2. b).

22 Art. 16 Amended Proposal COM(92) 422 final for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. C 1992,311/30, see Appendix VI. 2. c).

The EU Parliament added the rights "[t]o be informed of and to challenge the information and arguments used in the automatic processing whose outcome is detrimental to him".[23] The European Parliament accepted that there might be necessary automated decisions but tried to secure the position of the data subject. In the Council's version, the rule was framed first in a section conferring a right not to be subject to automated decisions and then in a second section describing the exceptions to that primary rule.

Several aspects of the explanations in the *travaux* are striking. In relation to its second draft, the European Commission states:

> "The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'".[24]

The European Commission acts upon the assumption that automation techniques would create a power imbalance between individuals and institutions and effectively exclude individuals from decision-making processes.

> "The danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities."[25]

What the statement implies might be more important than what it explicitly states. By framing it as a problem of the future, the Commission admits that it was not a problem at the time. The danger of misuses implies that there are also apt and legitimate uses. There is also a continuation of the *topos* of responsibility. Later, the Commission rules out that consent can be a legitimate exception to the prohibition of automation. While there is no justification of the discussions in the European Council, it has been reported that it was controversial whether to include a rule at all.[26] As a result of the process leading up to 95/46/EC, the original general prohibition in French law was turned into a more nuanced rule, applicable in cases of automated decisions based on processing of personal data and the evaluation of certain personal aspects. This rule had exceptions that were conditional upon the protection of the legitimate interests of data subjects.

---

[23] See Art. 15 Common position EC 95/C 93/01 for the text, see Appendix VI. 2. d).
[24] Art. 14 COM(90) 314 final, 29.
[25] COM(92) 422 final, 26 et seq.
[26] *U. Brühann* (note 19), 4.

It took almost twenty years until European institutions started to discuss an update to Directive 95/46/EC.[27] In the meantime, the Committee of Ministers of the Council of Europe issued a recommendation on profiling.[28] Profiling was also in focus for most of the legislative process. The Commission explicitly drafted a rule on profiling that differed regarding the exceptions in particular. It included individual consent, excluded specific categories of personal data and in the proposed recital the profiling of children. The European Parliament put much more emphasis on the protection of data subjects and included a general right to object to personal profiling. Whereas profiling leading to legal or substantial effects could be justified, this draft states in section 5 that profiling producing legal or significant effects

> "shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment".

This general prohibition of automated decisions is even stricter than the French law, considering that decisions predominantly based on automated means were also included. The substantive differences between Parliament and Commission could also be seen in the respective justifications. The substantive differences in the proposals of the European Commission and the European Parliament were not only restricted to automated decisions. For these and other reasons, a trilogue between those institutions and the Council was summoned in order to reach consensus. The ultimate rule on automation is indeed a compromise that again shifted its content substantially. The wording of Art. 22 GDPR only relates to automated decisions and leaves out profiling. Yet, there is an increased emphasis on the protection of the individual by adding the data subject's "rights and freedoms" to its legitimate interests. This could be conceived as a major shift extending the possible application of the regulation as well as the grounds to justify such a decision. The justification of the rule was also changed substantially: The regulation now deals not only with a projected future but also with emerging technologies that already have impacts. However, they are also projected to have beneficial consequences and are areas for further innovation.

---

[27] For an overview see *T. Weichert,* DSGVO Art. 22, in: W. Däubler/P. Wedde/T. Weichert/I. Sommer (Hrsg.). Kompaktkommentar, 2018, 324 (324).

[28] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23.11.2010 at the 1099th meeting of the Ministers' Deputies).

Considering the Commission had to argue in favour of a common market, it is understandable that the Commission aimed to avoid

> "hamper[ing] the development of useful services, but would also reduce citizens' willingness to use existing services when they fear becoming subject of constant monitoring of their lives".

This shows the remarkable transformation of a rule concerning automated decisions from a general prohibition based on future scenarios to a more and more general regulation distinguishing between lawful and unlawful uses of technologies. Changes in the regulation are seemingly also motivated by changes in the perception of technologies. The Commission sees the risks but also the potentials. This translates to a more nuanced regulation. One explanation for this differentiation is the fact that the functions of the law are more complex than just limiting technological developments.[29] The law can motivate the adoption of technologies. It also impacts and structures design processes. The evolution of Art. 22 GDPR reveals how this normative potential for motivation and design has opened up gradually. It shows how such a rule shifts between the different levels of government. It started from an isolated and singular rule in France. Through legislation in the European Union, this was turned on its head. Member states now had to legislate in order to make exceptions. It will be shown below that GDPR and Convention 108+, the updated version of Convention 108, have already led to a wider proliferation of the regulation of automated decisions.

III. Discursive Present: The Normative Potential in Academia and Practice

Art. 22 GDPR regulates automated decisions in four steps:[30] It first establishes a "right not to be subject to a decision based solely on automated processing" when this decision has legal or similar effect. It then defines three exceptions in section 2. It consequently spells out the requirements in which these exceptions apply in sections 2 and 3. Section 4 then contains a restriction for special categories of data. In the search for the normative potential of this regulation, one can look at the literature on Art. 22 GDPR and especially at academic discourses in order to understand the potential of the respective opinions. It is, however, also possible to discover uncharted

[29] On the function of the law regarding technology see *C. Djeffal* (note 3), 283 et seq.
[30] For the text of this provision see Appendix VI. 3. d).

potential of the regulation. In the latter regard, this article will argue that Art. 22 GDPR has not yet been fully appreciated, as it is actually a law-by-design clause that requires including not only legal but also societal concerns in the design of technology.

1. Unchartered Normative Potential: A Law-by-Design Obligation

The unchartered potential of Art. 22 GDPR lies in the fact that it is a law-by-design obligation.[31] The basic function of such an obligation is to mandate that legal values are to be realised in the process of inventing, adopting, designing, and using a system.[32] Instead of only regulating the use of technology, which is applying the law from the outside, law-by-design obligations aim to guide the whole socio-technical process of the creation and use of technology from the inside. The most common obligation addressing the design in European law is Art. 25 GDPR, which focusses on realising the principles of data protection as laid down in Art. 5 GDPR.[33] This contribution argues that Art. 22 GDPR is also to be read as a law-by-design obligation as it requires that automated decisions must contain "measures to safeguard the data subject's rights and freedoms and legitimate interests".[34] Instead of collecting enumerated rights, Art. 22 GDPR provides for an unenumerated rights approach that matches the impacts at issue with an adequate mix of measures. In doing so, it can avoid simply stating certain rights and looking into them in a tick-box manner. Instead, it is possible to find an adequate reaction for each situation based on the applicable rights, freedoms and legitimate interests. Designers on different levels have to internalise the respective legal values at issue in order to be able to strike

[31] The design aspect of Art. 22 GDPR is very briefly mentioned by *L. Moerel/M. Storm,* Automated Decisions Based on Profiling: Information, Explanation or Justification – That Is The Question!, in: N. Aggarwal/H. Eidenmüller/L. Enriques/J. Payne/K. van Zwieten (eds.), Autonomous Systems and the Law, 2019, 91.

[32] *M. Hildebrandt,* Saved by Design? The Case of Legal Protection by Design, in: Nanoethics, 2017, 307; *M. Hildebrandt,* Legal Protection by Design, Objections and Refutations, in: Legisprudence 5 (2015), 223.

[33] *M. Hansen,* Art. 25, in: S. Simitis/G. Hornung/I. Spiecker Döhmann (Hrsg.), Datenschutzrecht, 2019, 29 et seq.

[34] See generally *E. Gil González/P. D. Hert,* Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data – An Analysis of GDPR Provisions and Principles, in: ERA Forum, 2019, 597, 612.

this balance in practice. Those values go beyond data protection since Art. 22 GDPR addresses far more questions than that.

This reading is supported by the text of Art. 22 GDPR, especially the respective clause "measures to safeguard the data subject's rights and freedoms and legitimate interests" in Art. 22 GDPR. This is actually a general reference to all rights, freedoms, and legitimate interests. The term "measures" is also used in Art. 25 GDPR. While it is true that Art. 22 Sec. 3 GDPR contains a list of minimum requirements for the lawfulness of automated decision-making[35] and Recital 73 contains more, it is very clear from their wording that those mentions are non-exhaustive. As in many other cases of the GDPR, the purpose of Art. 22 GDPR is not limited to data protection. It is about protecting data subjects from unjust automated decisions impacting on their rights, freedoms and legitimate interests. Reading Art. 22 GDPR as law-by-design-obligation enhances the *effet utile* in two ways. It broadens the scope for all rights that are relevant. This is particularly important since digitisation is impacting ever more areas of life and, therefore, the areas of application cannot be limited to certain questions.[36] The open wording can also include group rights and collective rights if data subjects from respective entities holding these rights are affected.[37] Furthermore, to construct Art. 22 GDPR as law-by-design-obligation allows to address specific technical features. The way an automated system impacts rights and freedoms often depends on its specific socio-technical design. If Art. 22 GDPR has the aspiration to realise an all-encompassing protection as its text suggests, it is hard to see how this can be achieved by trying to limit and fix its content to certain preconceived rights like the right to transparency. This contribution, therefore, has to respectfully disagree with attempts to fix the content of Art. 22 GDPR and to come up with preconceived lists of rights.[38] While this might be valuable from a perspective of

35 It reads "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision".

36 *M. Hildebrandt,* Smart Technologies and the End(s) of Law, Novel Entanglements of Law and Technology, 2015.

37 Compare *S. Dreyer/W. Schulz,* The General Data Protection Regulation and Automated Decision-Making: Will It deliver?, Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole, 2019, 36. While they criticise Art. 22 GDPR for not addressing social and group issues. They do not touch upon its objective law-by-design nature that has the normative potential to include those concerns.

38 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6.2.2018, 32. *P. Voigt/A. v. d. Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), Praktikerhandbuch, 2018, 245.; *K. v. Lewinski,* DSGVO Art. 22, in: H. A. Wolff/S. Brink (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 2019, 1 (48 et seq.).

organising knowledge for a certain class of applications or an area of application, to fix the content of Art. 22 GDPR in advance would substantially hamper its ability to effectively safeguard data subjects.

A very good illustration of this point is the discussion whether Art. 22 GDPR contains a right to an explanation or transparency. Authors have provided many good arguments for or against a general right to a transparent decision in the context of Art. 22 GDPR.[39] However, even based on the state of the art today, it is clear that there is no valid one-size-fits-all answer to that question for ADMSs. In most cases, some form of transparency is necessary to safeguard human rights, however, it might also defeat the legitimate purpose of the automated decision. Take for example an automated decision by risk-management systems to detect tax fraud by singling out specific addresses for further review. If such a system were offering explanations, it could be possible to trick and circumvent it. The German Tax Code, therefore, provides for the secrecy of a risk management system; a right to explanation would undermine its purpose and impact on other constitutional values like fairness and tax justice. Thus, looking at the question of transparency from the perspective of law by design, the question must be whether transparency is safeguarding rights, freedoms, and legitimate interests better than other measures. This shifts the question from the existence of a right to transparency to the question how rights should be safeguarded effectively. In specific situations, independent oversight might be an even better solution. By constructing Art. 22 GDPR as law-by-design-obligation, one shifts the focus from preconceived rights to an exercise of weighing and balancing major consideration in the process of technology design.

In practice, organisations planning to install an ADMS will have to make sure that they know whether rights, freedoms and legitimate interests are at issue and include this into all stages of the process of drawing up and using the technology. Legal principles need to be an integral part of the process. While this assessment might be simple in well-known cases, in other cases where emerging capacities of AI are used, this is more complex. In these cases, a simple impact assessment might not be enough but there needs to be a deeper inquiry about the aspects of the technology. Such inquiries, which are often summarised with the umbrella term "responsible research and in-

[39] *B. Goodman/S. Flaxman,* European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation", in: AI Magazine 38 (2017), 50 (55); *S. Wachter/B. Mittelstadt/L. Floridi,* Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 2017; *L. Moerel/M. Storm* (note 31). The existence of a right to reveal the source code is discussed by *M. Martini,* Art. 22, in: B. P. Paal/D. A. Pauly (Hrsg.), Datenschutz-Grundverordnung, 2018, 36.

novation", all have in common that they transgress the ordinary methods of technology impact assessments.[40] In such cases, it is necessary to go beyond a data protection impact assessment as foreseen in Art. 35 GDPR. This is again a good example of the advantages of interpreting Art. 22 GDPR as law-by-design-obligation. It is more flexible, granular and allows to cover also problems raised by emerging technologies.

2. Contested Normative Potential

While the potential of Art. 22 GDPR as a law-by-design clause remains largely uncharted, commentators have highlighted many interpretive issues. The great range of interpretative possibilities is shown by contributions employing an extremely restrictive[41] or an extremely extensive[42] approach to interpretative questions in Art. 22 GDPR. As is often the case with new regulation, the jurisprudence of courts and future legislative activities might resolve such issues authoritatively. However, even in the face of such decisions, the normative potential uncovered by academic commentary remains important for the interpretation of the rule. In order to appreciate this potential, it is important to map the interpretative questions and the range of responses given to them.[43] Behind this dispute lies the question whether Art. 22 GDPR is rather a tool for empowerment of individuals in the face of automated decisions or a prohibition with immediate effect providing for a general framework.

[40] *J. Stilgoe/D. H. Guston,* Responsible Research and Innovation, in: U. Felt/R. Fouché/C. A. Miller/L. Smith-Doerr (Hrsg.), The Handbook of Science and Technology Studies, 2017, 853.; *A. Ely/P. van Zwanenberg/A. Stirling,* Broadening Out and Opening Up Technology Assessment: Approaches to Enhance International Development, Co-Ordination and Democratisation, in: Research Policy 43 (2014), 505.

[41] *S. Wachter/B. Mittelstadt/L. Floridi* (note 39), 90. The authors employ this restrictive approach in order to proof their hypothesis that there exists no right to a transparent decision.

[42] *B. Goodman/S. Flaxman* (note 39).

[43] For a more explicit methodology in that regard see *C. Djeffal,* Static and Evolutive Treaty Interpretation, A Functional Reconstruction, 2016, 76.

a) Prohibition or Right

Commentators have been quarrelling over whether Art. 22 GDPR is a prohibition or a right.[44] All agree that the provision confers a subjective right on the data subject since its wording is clear in that regard. However, they disagree whether there is also an objective function. This question has a huge impact on the normative potential of the provision. From a legal standpoint, one difference would be whether Art. 22 GDPR is only applicable when invoked by individuals or whether it applies automatically.[45] This difference is very significant for the law on the ground and the law in the books. The risk that action is taken against these controllers is substantially lower when it is dependent on individuals taking actions against a data breach. This might tempt many data controllers to breach the law with the hope that individuals will not make use of their rights. From a principal and jurisprudential standpoint, the alternative is between Art. 22 GDPR either giving rise to an isolated subjective right or being part of the objective framework guiding automated decisions generally and in every case. What might seem as a subtle difference in the first place is indeed a crucial distinction determining the scope and the normative potential of Art. 22 GDPR.

b) Decision

Most interpretative questions relate to the term "decision". There is agreement that a decision must be addressed with regard to individuals; however, there are many attempts to restrict the term. Behind those restrictive interpretations lies a specific view of automated decisions that requires protection by law. One could consider, for example the view that only complex automated decisions are addressed by Art. 22 GDPR.[46] One idea is to assume as an unwritten requirement that the decisions have to be based on processing relating to the personality of the data subject.[47] This would in effect include the phrase that was left out of the text as compared to Directive 95/46/EC. This has been criticised on the basis that the wording of the provision is clear and the dangers of profiling are thus present in the

[44] *S. Wachter/B. Mittelstadt/L. Floridi* (note 39), 94.; *L. A. Bygrave,* Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision Making, in: K. Yeung/M. Lodge (eds.), Algorithmic Regulation, 2019, 252.

[45] Open for this interpretation *S. Wachter/B. Mittelstadt/L. Floridi* (note 39), 94.

[46] *P. Scholz,* Art. 22, in: S. Simitis/G. Hornung/I. Spiecker Döhmann (note 33), 18.

[47] *K. v. Lewinski* (note 38), 7 et seq. For a detailed discussion see *L. A. Bygrave* (note 44), 252 et seq.

provision.[48] Looking beyond the specific legal arguments, the consequences for the normative potential are significant. A narrow reading would turn Art. 22 GDPR into a data-protection-specific provision protecting against profiling. Without the additional restriction, the same provision serves as a general rule for the admissibility of automated decisions. In this reading, Art. 22 GDPR goes far beyond the ambit of data protection.[49] Concerning automated decisions, the question is rather whether this is to be extended to situations in which there is only a formal but non-essential human intervention.[50] Several criteria are put forward to qualify decisions that are indeed taken by humans but must be classified as automated decisions: qualification and competence,[51] actual human influence,[52] *inter alia*. The normative potential of these views is to disqualify certain kinds of human involvement as insufficient. The opposite view stresses the sole human accountability even in those situations. One can reframe this issue as a question of an extension of responsibility for decisions despite the fact that certain people are nevertheless involved.

c) Decisions Significantly Affecting Data Subjects

Automated decisions only fall under Art. 22 GDPR if they have legal effects or if they affect the data subject in a significant manner. The latter alternative is again a contested concept. Some authors contend that only decisions having negative effects would qualify as significant.[53] Others do not assume this restriction.[54] This dissent again speaks to the general object and purpose of the whole provision. The question to be determined is whether

---

[48] *P. Scholz* (note 46), 19.; *M. Arning,* Kapitel 6, Umgang mit Betroffenen, in: F. Moos/J. Schefzig/M. Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, 2018, 141, 229.

[49] It is true that GDPR is only applicable when personal data are being processed according to Art. 2 GDPR *S. Dreyer/W. Schulz* (note 37), 18. However, it is hard to conceive any automated decision addressed at an individual that is meaningful and does not include any kind of information necessary to identify the data subject.

[50] *E. Gil González/P. D. Hert* (note 34), 613.

[51] *P. Scholz* (note 46), 27; *M. Martini* (note 39), 18 et seq.

[52] *G. Spindler/A. Z. Horváth,* DS-GVO Art. 22, in: G. Spindler/F. Schuster (Hrsg.), Grauer Kommentar, 2019, 1 (5); Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 6.2.2018, 21.

[53] *M. Arning* (note 48), 231; *B. Buchner,* DSGVO Art. 22, in: J. Kühling/B. Buchner/M. Bäcker (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2018, 473, para. 25; *P. Scholz,* § 6c, in: S. Simitis/U. Dammann/A. Arendt (Hrsg.), NomosKommentar, 2014, 35.

[54] *M. Martini* (note 39), 28.

the provision focuses on unjustified negative impacts or whether it follows a broader concept. A broader case might be focused on the potential of an ADMS to alter behaviour. This alternative also evades the question of what positive and negative effects actually mean and who should determine that. It speaks to a broader vision of checks and balances on measures that are able to guide human behaviour.

All in all, the above-mentioned arguments show how Art. 22 GDPR can be interpreted either broadly or narrowly. They convey different assumptions about the object and purpose of Art. 22 GDPR. In the restrictive readings, their potential lies in workable solutions evading unnecessary formalities in cases in which the rights, freedoms and legitimate interests of data subjects are not really at issue. In other cases, they seem able to extend to the scope of protection and address all kinds of automated decisions, irrespective of their generalised potential impact. Taken together, all those interpretative questions are part of a larger mosaic representing the issue of whether Art. 22 GDPR is a rather specific provision that is applicable only in certain cases or whether it is to be understood as a general rule. Thereby, every interpretative question determines the normative potential to some extent.

IV. Avenues for the Future: Comparative and Interdisciplinary Perspectives

1. Comparative Outlook

Will a national development impact data protection laws in Europe and beyond the same way that a French law has impacted data protection law in the past? A comparative look beyond the borders of the EU shows that there are original aspects in the legislation of some states.[55] Convention 108 offers an interesting sample as all members follow a general regulatory technique, while there is no explicit prescription on how to deal with automated decisions.[56] This sample also contains at least some variance consider-

[55] A study compared approaches in data protection laws of EU member states. *G. Malgieri,* Automated Decision-Making in the EU Member States, The Right to Explanation and Other "Suitable Safeguards" in the National Legislations, in: Computer Law & Security Review 35 (2019), 1. The study is, however, not consistent in that it looked into laws outside of data protection instruments in some countries while restricting the analysis to data protection law in others.

[56] So far, Convention 108+ has not become mandatory for any state.

ing that it covers states from Africa, Asia, and Latin America. How Convention 108 member states beyond the EU have been dealing with this issue varies considerably.[57] In states like Mexico,[58] Montenegro,[59] and Tunisia,[60] there is no rule on the issue. Other states have followed the initial French approach to ban automated decisions. That applies to Argentina,[61] Morocco,[62] and Senegal[63]. Albania,[64] Andorra,[65] Armenia,[66] Bosnia and Herzegovina,[67] and Monaco[68] have provisions that are identical with or very close to Directive 95/46/EC. Lichtenstein[69] and Mauritius[70] have synchronised their rule with Art. 22 GDPR. As for the future of data protection law, the most relevant question is which unique features states do provide for. The analysis of the legislation reveals the following specific aspects:

- Explicit prohibitions of discrimination
- Regulation of not fully automated decisions
- A right to objection
- An experimentation clause
- Transparency obligations.

Profiling leading to discrimination is explicitly prohibited in Lichtenstein's law.[71] The EU directive addressing data protection with regards to law enforcement authorities also contains a similar provision.[72] In Switzer-

57 Considering that there are many proposals for reform on the way, this analysis can only amount to a snapshot.

58 Data Protection Act 2017, <http://dataprotection.govmu.org>.

59 Personal Data Protection Law (2009, zuletzt geändert 2017), English translation <http://www.azlp.me>.

60 Loi organique numéro 63 portant sur la protection des données à caractère personnel (2004), <http://www.inpdp.nat.tn>.

61 Personal Data Protection Act 25.326 (2000), <https://rm.coe.int>. However, current reform proposal is very close to GDPR, see Art. 32 Mensjaje – Ley de Protección de Datos Personales, abrufbar unter: <https://www.argentina.gob.ar>.

62 Art. 11 Dahir No. 1-09-15 du 22 safar 1430 (2009), <https://www.cndp.ma>.

63 Art. 48 Loi No. 2008-12 sur la pro-tection des données à caractère personnel (2008), <https://www.wipo.int>.

64 Law No. 9887 on the Protection of Personal Data (2008), <https://www.afapdp.org>.

65 Art. 15 Decree of the Andorian Data Protection Authority 9-06-2010, based on Law 15/2003, Qualified Personal Data Protection Law (2003).

66 Art. 16 Law of Armenia on Protection of Personal Data (2015), <http://www.foi.am>.

67 Law on the Protection of Personal Data (2006), <https://www.refworld.org>.

68 Art. 22-1 Loi n. 1.353 du 04/12/2008 modifiant la loi No. 1.165 du 23.12.1993 réglementant les traitements d'informations nominatives, <https://www.legimonaco.mc>.

69 Art. 54 Data Protection Law (DSG 2018), <https://www.gesetze.li>, see reprint at VI. 4. a).

70 Data Protection Act 2017, <http://dataprotection.govmu.org>.

71 Art. 54 Data Protection Law (note 69).

72 Art. 11 Sec. 3 The Data Protection Law Enforcement Directive (EU) 2016/680.

land, there is a governmental experimentation clause for automated decisions concerning special categories of data.[73] Following the original French distinction, Morocco and Senegal prohibit judicial decisions based on automated systems, a category that also includes decision support systems. Based on its wording, the rule in Uruguay reaches even further and prohibits decisions with legal effects generally, which would include decision support systems.[74] Uruguay,[75] Azerbaijan,[76] and Switzerland[77] explicitly afford a data subject the right to object to automated decisions in a more general manner than Art. 22 Sec. 3 GDPR. The Russian provision adds procedural safeguards to this right.[78] Regarding transparency, most regulations are like Serbia's[79] in that they combine elements present in Arts. 13-15 and 22 GDPR. Judging from the text of the respective laws, only the Uruguayan law goes clearly beyond the text by requiring the controller to communicate the "valuation criteria" (*los criterios de valoración*).[80] Overall, there are selective differences where national laws of member states to Convention 108 clearly go beyond GDPR. Judging by the Convention text, Uruguay's adaptation has the most differences. However, most of its deviations are in the scope of what has been discussed in the processes finally leading up to Art. 22 GDPR.

2. New European Development

One important development in the regulation of automated decisions concerns the current discussions of regulating artificial intelligence on the European level. A series of documents have addressed the importance of artificial intelligence, the need to build a European ecosystem and the neces-

[73] Art. 17 and 17a Federal Data Protection Law, <https://www.admin.ch>.

[74] Art. 16 Sec. 1 Data Protection Act Law No. 18.331 (2008), <https://www.impo.com.uy>. Note, however, that Section 2 is only applicable to fully automated decisions.

[75] Art. 16 Sec. 2 Data Protection Act Law No. 18.331 (2008), <https://www.impo.com.uy>.

[76] Art. 7.3 Law No. 998-IIIQ on Personal Data (2010), <https://cis-legislation.com>, see reprint at VI. 4. b).

[77] Art. 11 Sec. 2 Federal Data Protection Law, <https://www.admin.ch>, see reprint at VI. 4. c).

[78] Art. 16 Sec. 3 Federal Law No. 152-FZ on Personal Data (2006), English translation <http://wko.at>, see reprint at VI. 4. f).

[79] Law on Personal Data Protection (2009), <https://www.poverenik.rs>, see reprint at VI. 4. g).

[80] Art. 16 Sec. 3 Data Protection Act Law No. 18.331 (2008), <https://www.impo.com.uy>, see reprint at VI. 4. h).

sity to develop a European approach concerning ethical, legal and social aspects.[81] In 2019, the European Commission emphasised AI as one of its key strategic issues and its regulation as one of the measures to be implemented.[82] It promised to put forward legislation within 100 days.[83] In 2020, the European Commission published a Whitepaper on AI in which it outlined important regulatory issues.[84] It started with general measures to boost the European AI ecosystem and then looked into regulation of AI. The Whitepaper addresses regulation from a classical standpoint, mitigating risks with new technologies in order "to protect fundamental rights (including personal data and privacy protection and non-discrimination), as well as safety and liability-related issues".[85] The Commission explicitly pointed to the increasing possibilities of automated actions and automated decisions. When analysing the human rights potentially impacted by AI, it mentioned that

> "the rights to freedom of expression, freedom of assembly, human dignity, non-discrimination […], as applicable in certain domains, protection of personal data and private life, or the right to an effective judicial remedy and a fair trial, as well as consumer protection".[86]

This extensive list begs the question, however, whether there is any human right that cannot be affected by AI. The EU Commission also highlighted transparency as an important prerequisite for the exercise of human rights.[87] It is also noteworthy that the EU Commission has so far abstained from symbolically proclaiming any new right but has instead opted to look into the protection of human rights as they stand in Europe.

As regarding the application of future regulation, the envisaged rules will also relate to systems that are not solely performing automated decisions. Accordingly, the types of requirements are broader. They include the following:

---

81 A regularly updated overview over all documents can be found at European Commission, Artificial Intelligence, Shaping Europe's digital future, 2020, <https://ec.europa.eu>.

82 *U.* von der *Leyen,* A Union that Strives for More My Agenda for Europe, Political Guidelines for the next European Commission 2019-2024, <https://ec.europa.eu>, 13.

83 *U.* von der *Leyen* (note 82), 12.

84 European Commission, White Paper On Artificial Intelligence, A European Approach to Excellence and Trust, 2020, <https://ec.europa.eu>. It was accompanied by European Commission, Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, <https://ec.europa.eu>.

85 European Commission (note 81), 10.

86 European Commission (note 81), 11.

87 European Commission (note 81), 13.

- "training data;
- data and record-keeping;
- information to be provided;
- robustness and accuracy;
- human oversight;
- specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification".[88]

The typology of the European Commission has its focus on how machine learning works. The different types of regulation are within the scope of measures of Art. 22 GDPR. This does not come as a surprise, given that Art. 22 GDPR does not really exclude any measure that helps to safeguard rights, freedoms and legitimate interests. What is new is the governance, compliance and enforcement dimensions explicitly introduced by the Whitepaper. In one sense, the European Commission is delivering on the promise given in Art. 22 GDPR. It also adds an objective dimension to Art. 22 GDPR and comparable rules in national law. It is not only on the individual to object and to enforce his or her rights, but the law provides for a governance framework that furthers the realisation of human rights. As regarding compliance and enforcement, the European Commission issued a large study in a separate report looking into several areas of regulation.[89] Regarding the governance of AI, the European Commission seems to have overcome the temptation to found a shiny new organisation. Instead, it invests in networking and knowledge exchange between different actors and authorities.[90]

This is in line with the general approach of the Commission to develop the European legal framework successively and incrementally. The emphasis on compliance, enforcement and governance are apt ways to show how AI development can be achieved in such a way that safeguards human rights, freedoms, and legitimate interests. While this is only a snapshot, the emphasis of a general and objective framework allowing for individual and collective realisation of constitutional norms is key to the whole endeavour of the European Commission. This would add to Art. 22 GDPR and similar norms and help to realise them, particularly if they constitute a law-by-design-obligation.

88 European Commission (note 81), 18.
89 European Commission, Report on the Safety (note 84).
90 European Commission, White Paper (note 84), 25.

V. Summary and Conclusion: The Normative Potential of Art. 22 GDPR

Art. 22 GDPR is one of the few rules that rather directly addresses AI systems. The preceding analysis revealed that Art. 22 GDPR is in effect a law-by-design-obligation. It requires developers to include the rights, freedoms, and legitimate interests of data subjects into the design process. In applying Art. 22 GDPR, it does not suffice to apply a predetermined set of rules. In contrast, one has to perform a socio-technical impact assessment and weigh and balance all aspects. This nature of the obligation has been achieved only after a substantial evolution from a flat-out prohibition in French law to a more nuanced approach in European law. The same evolution also led to a regional proliferation of the law concerning ADMSs, which might soon include not only member states of the Council of Europe but many states beyond the confines of Europe including African, Asian, and American states. In this constant evolution, international law like the Convention 108 of the Council of Europe sets general standards while European and national legislations keep pushing these standards further. A major legislative overhaul is to be expected on the European level. This overhaul will necessitate the acknowledgement of the normative potential of the provisions already in place. As shown in this article, interpretative choices allow us to construe this norm in a very different manner concerning its objective or subjective nature or its broad or narrow notion of what is a decision or the definition of how a data subject is to be affected. The way in which those and other interpretative disputes are settled shape the normative potential of Art. 22 GDPR. What is most significant, however, has neither been sufficiently recognised nor realised so far: its general nature as law-by-design clause.

VI. Appendix

1. French Data Protection Law

a) Art. 2 Draft Law No. 2516 of 9 August 1976 on Information Technology and Civil Liberties

Aucune décision juridictionnelle ou administrative impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations.

b) Art. 2 Act No. 78-17 on Information Technology, Data Files and Civil Liberties, Journal Officiel de la Republique Française 1978, 227

Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'interessé.

2. EU Data Protection Directive

a) Art. 14 No. 2 Commission Proposal COM(90) 314 Final for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, O.J. 1990, C 277/3

The Member States shall grant a data subject the following rights: [...]

2. Not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality.

b) Amendment No. 46 Opinion of the European Parliament 0314 – C3-0323/90 on the Proposal for a Directive I COM(90), O.J. 1992, C 94/173

[The Member States shall grant a data subject the following rights:]

2. Not to be subject to an administrative or private decision involving an assessment of his character which has as its sole basis the automatic processing of personal data defining his profile or personality, save where the data subject has requested or given his consent to such assessment in accordance with the provisions of Article 12 or in the circumstances described in Article 8(1)(-a) and (a).

2a. To be informed of and to challenge the information and arguments used in the automatic processing whose outcome is detrimental to him.

c) Art. 16 Amended Proposal COM(92) 422 final for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. C 1992, 311/30

1. Member states shall grant the right to every person not to be subjected to an administrative or private decision adversely affecting him which is based solely on automatic processing defining a personality profile.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided any request by the data subject has been satisfied, or that there are suitable measures to safeguard his legitimate interests, which must include arrangements allowing him to defend his point of view; or

(b) is authorized by law which also lays down measures to safeguard the data subject's legitimate interests.

d) Art. 15 Common Position (EC) No 1/95 with a View to Adopting Directive 95/.../EC of the European Parliament and of the Council of ... on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. 1995 C 93/1

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request by the data subject has been satisfied, or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to defend his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

e) Final Version: Art. 15 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. 1995, L 281/31

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

3. EU General Data Protection Regulation (GDPR)

a) Art. 20 Commission Proposal COM/2012/011 final for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. 2012, C 102/24

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria

and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

b) Art. 20 European Parliament Legislative Resolution P7_TA(2014)0212 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. 2017, C 378/55

1. Without prejudice to the provisions in Article 6, every natural person shall have the right to object to profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.

2. Subject to the other provisions of this Regulation, a person may be subjected to profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject only if the processing:

(a) is necessary for the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied, provided that suitable measures to safeguard the data subject's legitimate interests have been adduced; or

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9.

5. Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The suitable measures to safeguard the data subject's legitimate interests referred

to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.

5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.

c) Art. 22 Position No. 6/2016 of the Council at First Reading with a View to the Adoption of a Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, O.J. 2016, C 159/1

1. 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.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article (1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

d) Final Version: Art. 22 Regulation 679/2016/EU on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, O.J. 2016, L 119/1

1. 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.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4. National Laws

a) Principality of Liechtenstein Data Protection Act of 4 October 2018, Official Gazette No. 2018.272

Art. 54

Automatisierte Einzelentscheidung

1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn dafür eine gesetzliche Grundlage besteht.

2) Entscheidungen nach Abs. 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum

Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

b) Republic of Azerbaijan Law No. 998-IIIQ of 11 May 2010 on Personal Data, Collection of Laws of the Republic of Azerbaijan No. 6(156), Section 480 (Status as of 3 April 2018) (Unofficial Translation by the Azerbaijani State Committee for Family, Women and Children Affairs)

Art. 7.3

In the event that [the] decision talen [taken] as a result of [the] collection and processing of personal data through information technologies breaches [violates the] interests of the subject entity, he/she shall be entitled to object against [the] collection and processing of such data by means of mentioned metho[ds], except for cases which are of mandatory nature, as provided for in the legislation. In the event that [the] owner or operator receives an objection against processing of persobal [personal] data through information technologies, they shall be obliged to receive [obtain] consent of the subject entity for [the] processing of data through the other method or to suspend processing of personal data immediately.

c) Swiss Federal Act on Data Protection of 19 June 1992 (Status as of 1 March 2019)

Art. 17: Legal Basis

1. Federal bodies may process personal data if there is a statutory basis for doing so.

2. They may process sensitive personal data and personality profiles only if a formal enactment expressly provides therefor or if, by way of exception:

(a) such processing is essential for a task clearly defined in a formal enactment;

(b) the Federal Council authorises processing in an individual case because the rights of the data subject are not endangered; or

(c) the data subject has given his consent in an individual case or made his data general accessible and has not expressly prohibited its processing.

d) Kingdom of Morocco Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data and its implementing Decree No. 1-09-15, Bulletin Officiel No. 5714, 345

Article 11 : Neutralité des effets

1. Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

2. Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

3. Ne sont pas considérées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.

e) Republic of Senegal Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data, Journal Officiel 2008, No. 6406

Art. 48

1. Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

2. Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

3. Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé des données à caractère personnel, les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations ni celles satisfaisant les demandes de la personne concernée.

f) Russian Federal Law No. 152-FZ of 27 July 2006 on Personal Data

Art. 16: Rights of Data Subjects in Relation to Decision-Taking Solely on the Basis of Automated Processing of Their Personal Data

1. It shall be prohibited for making decisions which give rise to legal consequences for a personal data subject or otherwise affect his rights and legitimate interests to be taken solely on the basis of the automated processing of personal data, except in the instances envisaged by part 2 of this Article.

2. A decision which gives rise to legal consequences for a personal data subject or otherwise affects his rights and legitimate interests may be taken solely on the basis of the automated processing of his personal data only if the subject of the personal data has given his written consent or in instances envisaged by federal laws which also establish measures to safeguard the rights and legitimate interests of the subject of the personal data.

3. An operator shall be obliged to make clear to a personal data subject the procedure whereby a decision is taken solely on the basis of the automated processing of his personal data and the possible legal consequences of such a decision, to allow him the opportunity to present an objection against such a decision, and to explain the means by which the personal data subject may protect his rights and legitimate interests.

4. An operator shall be obliged to consider an objection such as is referred to in part 3 of this Article within thirty days from the day of receiving it, and to notify the personal data subject of the results of the consideration of that objection.

g) Republic of Serbia Law on Personal Data Protection

Art. 9: Decision made by Automated Processing

1. Any decision producing legal consequences for a person or compromising his/her position cannot be based solely on data processed automatically and used in the assessment of some specific characteristic of his/hers (work ability, reliability, creditworthiness etc.).

2. Decisions referred to in paragraph 1 of this Article can be made where expressly provided for by the law or when a person's request relating to contract execution or performance is adopted, provided that adequate safeguards are put in place.

3. In cases referred to in paragraph 2 of this Article, the person concerned must be informed of the automated data processing and the decision-making process.

h) Oriental Republic of Uruguay Data Protection Act No. 18.331 of 18 August 2008

Art. 16: Derecho a la impugnación de valoraciones personales

1. Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.