BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 8 • N° 32 • DECEMBER 2022

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

HUMANS IN THE GDPR AND AIA GOVERNANCE OF AUTOMATED AND ALGORITHMIC SYSTEMS. ESSENTIAL PRE-REQUISITES AGAINST ABDICATING RESPONSIBILITIES

by Guillermo Lazcoz and Paul de Hert

The GDPR mandates humans to intervene in different ways in automated decision-making (ADM). Similar human intervention mechanisms can be found amongst the human oversight requirements in the future regulation of AI in the EU. However, Article 22 GDPR has become an unenforceable second-class right, following the fate of its direct precedent -Article 15 of the 1995 Data Protection Directive-. Then, why should European policymakers rely on mandatory human intervention as a governance mechanism for ADM systems? Our approach aims to move away from a view of human intervention as an individual right towards a procedural right that is part of the culture of accountability in the GDPR. The core idea to make humans meaningfully intervene in ADM is to help controllers comply with regulation and to demonstrate compliance. Yet, human intervention alone is not sufficient to achieve appropriate human oversight for these systems. Human intervention will not work without human governance. This is why DPIAs should play a key role before introducing it and throughout the life-cycle of the system. This approach fits better with the governance model proposed in the Artificial Intelligence Act. Human intervention is not a panacea, but we claim that it should be better understood and integrated into the regulatory ecosystem to achieve appropriate oversight over ADM systems.

Keywords: Human oversight; GDPR; Human intervention; Artificial intelligence; Accountability

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
This is a first draft working paper; the final version to be published in Computer Law & Security Review, for the forthcoming special issue on «EU Data legislative revolution: the ethical issues that still remain».

Disclaimer

1. Introduction: Human intervention will not work without human governance!

Automated decision-making systems (ADM) are hybrid systems, involving human and artificial agents in a particular socio-technological framework.[1] The proliferation of artificial intelligence (AI) technologies in our society is driving the automation of decision-making in more and more domains. As AI technologies evolve and become more effective, there is an increasing reliance on delegation of tasks coupled with an expectation of trust in such delegation.[2] This delegation process results in a restricted human intervention that is limited to the ex-ante programming activities and the ex-post observations of the results.[3] Nonetheless, as Citron and Pasquale explained for credit score systems, ADM systems that are sovereign over important aspects of our lives should not proceed without human intervention at all[4]. As we have explained elsewhere,[5] achieving an adequate level of oversight that holds humans accountable is the main reason for having a human intervene in the machine decision loop. The idea is propelled by the second paragraph of Art. 5 of the EU General Data Protection Regulation (GDPR) (on the principles of data protection) stating that 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')'.

However, this idea of intervening in the world of machines, as logical as it fits the GDPR, can take different forms and evolves as technology does. Some legislations have relied on mandatory human intervention as a governance mechanism, introducing –in different ways– a human agent in the decision-making process. Article 22 GDPR requires human intervention especially when automated processing involves the evaluation of personal aspects of the data subject: for some automated decisions human intervention is required as an essential component of decision-making [article 22(1) GDPR-decisions/*human in the loop decisions*], for others human intervention is only a safeguard on request [article 22(2) GDPR-decisions/ *human out of the loop decisions/ human on request decisions*].

These governance mechanisms remain underdiscussed in the legal analysis of the GDPR, where most energy seems to go to the transparency requirements at the cost of other requirements in Article 22 GDPR. Yet, similar human intervention mechanisms seem to come to the fore when discussing mandatory human oversight requirements in the future regulation of AI in the EU. In our opinion, human intervention as governance mechanisms demands for a more in-depth analysis. Our approach aims to move away from a view of human intervention as an individual right, towards a procedural right that is part of the culture of accountability in the GDPR. However, and at the same time, we argue that human intervention alone is not sufficient to achieve appropriate human oversight for these systems. Human intervention will not work without human governance.

This renewal interest for a human intervention requirement, propelled by the proposed EU regulation on AI (see *below),* urges to look back on some of the criticisms in literature against human intervention as an effective safeguard. What we are witnessing is not that key decisions are delegated to machines with no human in the loop; rather, that people making pressured decisions are presented with empirical

1 Matthias Spielkamp (Ed.), 'Automating Society. Taking Stock of Automated Decision-Making in the EU' (2019) 9.
2 Mariarosaria Taddeo, 'Trusting Digital Technologies Correctly' (2017) 27 Minds and Machines 565, 566.
3 Salvatore Sapienza, 'Ethical Perspectives on Big Data in Agri-Food: Ownership and Governance for Safety' (Università di Bologna 2021) 173.
4 Danielle Keats Citron and Frank A Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1, 7–8.
5 Paul de Hert and Guillermo Lazcoz, 'When GDPR-Principles Blind Each Other. Accountability, Not Transparency, at the Heart of Algorithmic Governance' (2022) Forthcoming European Data Protection Law Review.

rankings of risk, whose rationale they have no way of questioning.[6] The problem exists for most DM systems, regardless of whether the system is fully automated or includes human intervention.[7] Among other limitations, the influence of automation bias on human agents poses several restrictions for their intervention to be meaningful. Some authors therefore insist that we cannot systematically rely upon human agents to overcome or mitigate the concerns associated with ADM systems.[8] When discussing human intervention governance mechanisms in the GDPR, our contribution aims to address its limitations.

The structure of this paper is the following. In section 2 we first briefly introduce the content of Article 22 GDPR and discuss the lack of legal success of its direct precedent -Article 15 of the 1995 Data Protection Directive-. Are the ideas in these provisions unenforceable? Are these provisions second-class data protection rights?

Next, we look at what is the role of human intervention in the proposed AI regulation and how is it related to Article 22 GDPR (section 3). Section 4 deals with the White Paper on AI that explains more in detail how human intervention governance mechanisms, like the ones introduced in the GDPR, can serve to achieve appropriate human oversight for high-risk AI systems.

In sections 5, 6, and 7 we go back to Article 22 GDPR to understand its two human intervention governance mechanisms: an essential component of decision-making for 22(1) decisions (section 6) and a safeguard on request for 22(2) decisions (section 7). Next, following Article 29 Working Party's interpretation and recent judgments, we argue that the kind of human intervention required by the GDPR should be *meaningful* (section 8). However, much work remains to be done on what should be understood as meaningful human intervention. With this in mind, we approach the Commission's preparatory work for the 1995 Directive. There we find that one of the grounds for human intervention is the contestability of decisions by the data subjects they affect (section 9). But more important is the second ground analysed in section 10, the regulation introduces human intervention to make data controllers responsible for the processing of data. This is, where ADM takes place, humans help controllers to comply with the regulation and to demonstrate compliance. We then show how this tie between human intervention and accountability fits into the systemic governance regime of the GDPR through Data Protection Impact Assessments (sections 11 and 12). Despite their limitations, these tools can provide a continuous evaluation of human intervention that enables the controllers to demonstrate that the human intervention is meaningful in compliance with the GDPR. To conclude, we analyse a likely scenario that data controllers would face if they found that human intervention is meaningless in their ADM systems (section 13).

From an individual rights perspective, human intervention does not seem to provide satisfactory solutions for the governance of algorithmic systems. Yes, the general prohibition in 22(1) GDPR ensures the presence of a human in the loop for data subjects.[9] And when the prohibition is circumvented by one of the legitimate exceptions, the data subject may require the intervention of a human out of the loop. Yet, this perspective tells us little about the meaningfulness of that intervention and its influence on data processing. But if we shift our perspective to the systemic governance of the GDPR built on the accountability principle, the picture changes.

6 Dan McQuillan, 'The Political Affinities of AI' in Andreas Sudmann (ed), *The Democratization of Artificial Intelligence: Net Politics in the Era of Learning Algorithms* (transcript Verlag 2020) 165.
7 Danielle Keats Citron, 'Technological Due Process' (2008) 85 Washington Law Review 1249, 1267.
8 Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation and Governance 505, 516.
9 Even if that human in the loop is invisible for data subjects, since there is no individual right that informs or gives access to humans in the loop that avoid decisions based solely on automated processing.

What we propose is an evidence-based understanding of human intervention: (1) There is a place for meaningful and accountable human intervention in the GDPR and it can be enforced; (2) The delegation of tasks on sophisticated machines transforms the possibilities of human intervention, but it does not imply that humans should not have an oversight-role at all; (3) Data Protection Impact Assessments introduce obligations on controllers regarding human intervention, with a sufficiently wide margin of discretion for compliance to provide for evidence-based intervention; (4) Human intervention is not a panacea, and it will not work without further human governance, its implementation and assessment must be understood in connection to the rest of the GDPR regulatory ecosystem.

2. Article 22 GDPR, Swiss cheese addressing Kafkaesque dehumanisation

Article 22 GDPR:

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.

The first paragraph of Article 22 GDPR prohibits[10] ADM without human intervention[11] (including profiling)[12] that produces legal or significant effects on the data subjects.[13]

10 According to the extinct Article 29 Working Party (WP29) in its 2017 (last revised and adopted in 2018) Guidelines and interpreted equally consistently by the legal literature -not without some exceptions, see Luca Tosoni, 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' [2021] International Data Privacy Law.-, this is a general ban on fully automated decision-making and not a right to be actively exercised by the data subject. The interpretation of 22(1) GDPR as a general prohibition is also followed in recent judgments by the Hague and Amsterdam District Courts in the cases mentioned bellow.

11 This aspect is key to our analysis: the prohibition is about decisions *based solely on automated processing*. It seems obvious that decisions taken automatically, without any human intervention, are based solely on automated processing. However, what about decisions where the role of human agents is limited to rubberstamping the machine's output? Against these cases, one needs to address *the threshold of minimum human intervention* required not to make a decision-making 'solely' automated, Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243, 244. That is what we do in section 8.

12 Profiling plays a key role in the regulation of ADM systems in the GDPR, yet the prohibition applies whether or not the automated processing entails profiling according to art. 4(4) GDPR. Nor does this key role mean that every automatically produced profile falls within the scope of Article 22's prohibitions. For example, profiling is not affected by the 22(1) prohibition where it is intended as a decision support for a human operator, or where it produces no legal or similarly significantly affecting effects on the data subjects.

13 The distinction between decisions that produce legal or significant effects is very relevant from the point of view of the right to privacy and data protection. As we will see below, the distinction between 22(1) and 22(2) decisions based on prior human intervention in ADM has relevant legal consequences, yet it is the production of legal or meaningful effects in automated

The second paragraph formulates three exceptions to this prohibition: solely automated processing activities are possible in the case of contractual necessity, consent and authorisation by EU or Member State Law (Article 22(2) GDPR). These exceptions to the prohibition can only be invoked when measures to safeguard the data subject's rights and freedoms and legitimate interests are present.[14] For the two first exceptions, -contractual necessity and consent-, those safeguards must include, at least, the rights to obtain human intervention, to express his or her point of view and to contest the decision (22(3) GDPR).[15] The third exception -activities made possible by authorisation by EU or Member State-, is vaguely drafted: the GDPR is silent on what kind of safeguards can be 'suitable' to allow this exception to be invoked.[16]

The fourth paragraph contains a specific prohibition with regard to the automated decisions made possible under the three exceptions: these cannot use sensitive categories of personal data listed in art. 9(1) GDPR (data on health, on sexual orientation or ethnic origin, among others). However, this specific prohibition is lifted when automated decisions based on sensitive data are based on explicit consent (9(2)(a) GDPR) or 'reasons of substantial public interest' based on Union or Member State law (9(2)(g) GDPR).

Due to its broad limitations and exceptions, Article 22 GDPR has been compared with Swiss cheese and its giant holes.[17] But the main idea stands: humans should not be enslaved to machines and their decisions. Article 22 GDPR is a vivid example of how the Europeans have imposed restrictions on fully automated processing for computational technologies, drawing important bright line rules on what it means to be a human through the regulatory figure of the human in the loop and other analogous mechanisms.[18] Similar

processing -and not human intervention- what determines the interference with the right to privacy. This same argument seems to be held by the Hague District Court in a case brought by several civil society NGOs, concerning SyRI (Systeem Risico Indicatie), a data-driven instrument used by the Dutch government to detect and combat fraud with social benefits, allowances and taxes, Judgment of 5 February 2020 (C/09/550982 / HA ZA 18-388), paragraph 6.60: *The court does not give an opinion on whether the exact definition of automated individual decision-making in the GDPR and, insofar as this is the case, one or more of the exceptions to the prohibition in the GDPR have been met. That is irrelevant in the context of the review by the court whether the SyRI legislation meets the requirements of Article 8 ECHR. However, the court does consider the aforementioned significant effect of the submission of a risk report and its inclusion in the risk reports register on the private life of the data subject a significant factor in its assessment whether the SyRI legislation meets the requirements of Article 8 paragraph 2 ECHR. This effect, too, determines in part the extent to which the SyRI legislation interferes with the right to respect for private life*. [Official English version of the judgment]

14 The Italian DPA -*Garante per la protezione dei dati personali*- fined the digital platform, Foodinho, €2,600,000 for using discriminatory algorithms to manage its food delivery riders. Among other violations, the DPA considered that the company did not take the appropriate measures set out in Article 22(3) for ADM on the basis of one of the exceptions in Article 22(2), in this case, contractual necessity. See Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Foodinho s.r.l., 10th June 2021 [9675440].

15 As will be described in sections 5 and 7, paragraph 22(2)-decisions contain human intervention as a safeguard, a human out of the loop on request.

16 Through their National Laws implementing the GDPR, Member States have adopted different approaches for the exception contained in art. 22(2)(b), not only developing different suitable measures to safeguard the data subject's rights but also interpreting in different ways the possibilities that this exception offers to broaden ADM. See Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' [2019] Computer Law & Security Review.

17 Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond' (2019) 27 International Journal of Law and Information Technology 91, 95. Somewhere else we propose some clarifications and changes to improve Article 22 GDPR. Paul de Hert and Guillermo Lazcoz, 'Radical Rewriting of Article 22 GDPR on Machine Decisions in the AI Era' (*European Law Blog*, 2021) <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/>.

18 See Meg Leta Jones, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216. The human in the loop is the most common kind of governance mechanism based on human intervention, but not the only one. See the examples provided by the White Paper on AI in section 4.

provisions were rightly added in the 2016 Directive on Data Protection and Law Enforcement,[19] and the Directive on Processing of Passenger Name Record Data.[20]

Article 22 GDPR remounts to Article 15 of the 1995 *Directive on the protection of individuals with regard to the processing of personal data* (Directive 95/46/EC; no longer in force). Solove refers to this older provision as an example of how European regulators were already in the nineties recognising some of the dimensions of what he defined as the *database privacy problem*, which was neglected by US privacy law at that time.[21] In his view, the database privacy problem represents a form of dehumanisation that exacerbates the disempowering effects of bureaucracy,[22] a form of dehumanisation depicted in *The Trial*, Franz Kafka's novel. In this novel, an ordinary person –Joseph K.– is arrested on his 30th birthday and, from then on, condemned to deal with an unreasoning and unreasonable authority.[23]

So, Article 15 of the 1995 Directive pioneered in this area. However, the provision was *rarely enforced, poorly understood and easily circumvented*.[24] Some conceived it as a second-class data protection right that remained *largely dormant*.[25] Considering such precedent, one of the most important challenges concerning Article 22 GDPR would be to turn it into a first-class data protection right, fitting neatly into the systemic governance regime of the GDPR. To date, these provisions never figured centrally in litigation before the Court of Justice of the EU (CJEU) and relevant precedents in national courts are also scarce.[26]

Will Article 22 GDPR follow a different path than its precedent? There are grounds for optimism.
Article 22 GDPR and the Article 29 Working Party's guidelines interpreting it,[27] have at least raised a prolific academic discussion. Unfortunately, in our view, this discussion mainly focused on explainability and transparency-aspects of ADM in the GDPR. The GDPR governance model insists on transparency duties but goes beyond it by providing additional legal solutions and safeguards, among others, the one that is central here: human intervention. As explained in the introduction to this contribution, we miss a debate

19 Directive (EU) 2016/680. Article 11(1): Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

20 Directive (EU) 2016/681. Article 7(6): The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

21 Daniel J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stanford Law Review 1393, 1460.

22 ibid 1424. McQuillan holds that like bureaucracy in the twentieth century, AI is poised to become the unifying logic of legitimation across corporations and government, McQuillan (n 6) 165.

23 This metaphor was later picked up by other legal scholars that christened Article 15 as the Kafkaesque provision, a term now extended to its successor, Article 22 GDPR. Among others, Mireille Hildebrandt, 'Technology and the End of Law' in Erik Claes, Wouter Devroe and Bert Keirsbilck (eds), *Facing the limits of the law* (Springer 2009); Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233; Frederik J Zuiderveen Borgesius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24 The International Journal of Human Rights 1.

24 Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling BT -' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer International Publishing 2017) 78.

25 Lee A Bygrave, 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision-Making' in Karen Yeung and Martin Lodge (eds), *Algorithmic Regulation* (Oxford University Press 2019) 1.

26 In addition to the precedents mentioned in this section, a summary of the few precedents can be found in Antoni Roig, *Las Garantías Frente a Las Decisiones Automatizadas. Del Reglamento General de Protección de Datos a La Gobernanza Algorítmica* (Bosch Editor 2020).

27 The Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 were first adopted on 3 October 2017, and last revised and adopted on 6 February 2018. During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines. Endorsement 1/2018, see: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_es

on this aspect of Article 22 GDPR unserved by literature.[28] This might change, with the appearance of human intervention as an essential safeguard in the regulatory model for AI proposed by the European institutions.

3. Human intervention in the proposed Artificial Intelligence Act

Over the last few years, the European institutions have expressed their interest in strengthening the regulation of artificial intelligence technologies, addressing the call for a more transparent, robust, holistic and coherent system for regulating the development and use of such technologies.[29] This agenda is fuelled by the feeling that the GDPR and other laws in place remain sub-optimal on several fronts.[30]

The main outcome of the mentioned interest in strengthening the current legal framework is the *Regulation laying down harmonised rules on artificial intelligence* by the Commission (the proposed 2021 Artificial Intelligence Act (AIA)).[31] The path that preceded this outcome is also relevant to our analysis. In 2018, the Commission made public the European Strategy on AI.[32] In parallel, a *Coordinated Plan on AI* was published in December 2018 as a joint commitment with Member States.[33] A *high-level expert group on artificial intelligence* (AI HLEG) was appointed to provide advice on the European Strategy on AI, and its deliverables served as resources for new policymaking initiatives.[34] Among them, in February 2020, *the White Paper on Artificial Intelligence*[35] was published by the Commission. The White Paper defined an ecosystem of trust in which a regulatory framework for IA should be promoted to address the opportunities and risks of these technologies._More recently, the European Parliament's ambitious resolution of 20 October 2020 included a proposal for a *Regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies*.[36] In what follows, we only look at these policy documents and proposals from the perspective of Article 22 GDPR.

Both the Commission and the Parliament in their earlier 2020 statements gave a key role to human oversight for the development and use of AI. The respective documents consider that human oversight

28 Aziz Z Huq, 'A Right to a Human Decision' (2020) 106 Virginia Law Review 611, 624.
29 Julia Black and Andrew D Murray, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10 European Journal of Law and Technology 1, 16.
30 Raphaël Gellert, 'Comparing Definitions of Data and Information in Data Protection Law and Machine Learning: A Useful Way Forward to Meaningfully Regulate Algorithms?' (2020) n/a Regulation & Governance 16.
31 European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final. Our analysis of this proposal is quite positive as far as human supervision is concerned. However, we recommend the critical reading of other aspects of the proposal by Veale and Zuiderveen Borgesius that are not addressed in this paper. See Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97.
32 European Commission, Artificial Intelligence for Europe, COM (2018) 237 final.
33 European Commission, Coordinated Plan on Artificial Intelligence, COM(2018) 795 final. This plan was renewed by the Coordinated Plan on Artificial Intelligence 2021 Review, COM(2021) 205 final.
34 The most relevant deliverable in this regard are the Guidelines for Trustworthy AI in 2019. See European Commission, Building Trust in Human Centric Artificial Intelligence, COM(2019) 168 final.
35 European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final.
36 European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

needed to be mandatory for high-risk AI.[37] Both documents also insist on human oversight for the development and use of *human-centric AI*,[38] a notion that did not make it in the 2021 proposal for the Artificial Intelligence Act.[39] However, the essence is there: the proposed Act establishes human oversight as one of the mandatory requirements for high-risk AI (articles 8(1) and 14 AIA).

Interesting in comparison with the GDPR is how this proposed Act defines the key participants across the AI value chain. Looking at the definitions in Article 3, we learn that *development phase* and *use phase* are the two main phases in the AI lifecycle, whose key participants are *providers*[40] and *users*[41] respectively. For our analysis it is relevant to note that the algorithmic issues and safeguards related to Article 22 GDPR only address the second stage of AI use.[42] Hence, the AIA proposal, on this important point, goes beyond the GDPR and states that already in the first stage of development appropriate human oversight measures and duties should be identified and implemented by the provider (Recital 48 AIA):

> *(48) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role*

37 On the one hand, the White Paper states that high-risk AI applications should be subject to mandatory legal requirements, which include human oversight. On the other hand, ethical principles regulated as obligations, human-centric AI among them, should only apply to high-risk AI technologies according to the Parliament's proposal for a Regulation on ethical principles. Note that both documents offer a different qualification of what is high-risk. Regarding how high-risk is assessed, the Parliament's proposal for a Regulation on ethical principles risk assessment could be considered an improved version of the model proposed in the White Paper. The latter took into account two cumulative factors: the sector in which the application is employed, and the potential risks associated with the specific use of it, European Commission (n 34) 17. While the former divides them into three cumulative factors and the first two are enumerated in a *numerus clausus* list: the sector where they are developed, deployed or used, their specific use or purpose and the severity of the injury or harm that can be expected to occur should be considered (Recital 11). Finally, even if -following its precedents- the AIA includes a list of sectors and intended uses that shall also be considered high-risk (article 6(2) and Annex III), the general rule seeks to harmonise existing product safety legislation. As stated in article 6(1) AIA, the AI systems intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation (Annex II), shall be considered high-risk if they are required to undergo a third-party conformity assessment under that legislation.

38 According to the 2020 White Paper, an appropriate involvement by human beings –an appropriate human oversight– is necessary to achieve human-centric AI, European Commission (n 34) 21, while in the Parliament's proposal for a Regulation on ethical principles, human-centric AI as an ethical principle means that AI needs to be developed, deployed and used in a manner that guarantees full human oversight at any time (article 7(1)), including the possibility of regaining human control at any time (article 7(2)), and should be meaningful irrespective of the specific manifestation adopted –human review, judgment, intervention or control– (Recital 10).

39 Human-centric AI as a regulatory goal was dismissed by the Artificial Intelligence Act. In the Explanatory Memorandum, the call for a human-centric AI was replaced for the call for human centric rules for AI: *Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be human centric, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights (p.1).*

40 Article 3(2) AIA 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

41 Article 3(4) AIA 'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;

42 Gellert (n 30) 16. The first *development*-stage is indeed out of the GDPR scope when it comes to providing governance mechanisms for automated decision-making, just as this important stage remained beyond the scope of legal scholars' analysis and policy solutions, David Lehr and Paul Ohm, 'Playing with the Data: What Legal Scholars Should Learn about Machine Learning' (2017) 51 UC Davis Law Review 653, 655. According to Almada, this is a narrow interpretation of the GDPR *that restricts intervention to the end stages would make it useless, but human intervention in the design stages may be more effective by proposing alternative models of the data that take such concerns into account*, Marco Almada, 'Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems', *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (ACM 2019) 5.

These duties for the providers are further elaborated in Articles 13, 14, 16 and 29 of the AIA text. Providers shall ensure high-risk AI systems are compliant with the human oversight requirement (16(a) AIA). To comply with this requirement, they have to design and develop AI systems in a way that they can be effectively overseen by human agents during the use stage (14(1) AIA).[43] Before placing the AI system on the market, the providers either identify the appropriate measures to be implemented by the user, or identify and build them, when technically feasible into the system (14(2) AIA). Such measures shall enable human agents -to whom human oversight is assigned- to understand the capacities and limitations of the system, to correctly interpret its outputs, or to interrupt the system, among others, in the use stage (14(4) AIA).[44]

To these duties to make AI-oversight possible, one need to add the transparency requirements laid down in Article 13 AIA,[45] and the obligations for users of high-risk AI systems anchored in Article 29 AIA. This last provision states that users shall utilise the information provided by the provider about human oversight measures to comply with their obligation to carry out a Data Protection Impact Assessment under Article 35 GDPR (29(6) AIA).

Article 29 AIA shows a remarkable effort to bring the proposed regulation on AI in line with the GDPR.[46] This effort by the Commission is evidenced when comparing the Artificial Intelligence Act with the White Paper on AI. This comparison will show how the interesting insights on human oversight in the light of Article 22 GDPR described by the White Paper are further developed in the AIA, by providing legal safeguards for the design and development stages of AI systems that are not only remarkable, but also compatible with the GDPR.

4. Comparing the Artificial Intelligence Act with the White Paper on AI

We already sketched the role of the 2020 Commission White Paper on AI that developed the idea of mandatory human oversight for high-risk AI systems. When conceptualizing this idea and putting it forward in the Paper, the Commission came up with human intervention mechanisms that look familiar from the Article 22 GDPR-perspective.[47] The White Paper discusses various high-risk AI applications and proposed different types and degrees of human involvement depending on the intended use of the AI and its potential effects.[48] So human oversight, as it is called in the White Paper, is not a one size fits

43 The Commission understands that the concept of human oversight focuses on the human agent interpreting and following or modifying the output at the use stage. This implies that 'oversight' as a requirement does not extend to concepts such as organisational oversight, although we can also qualify it as 'human' in a broad sense.

44 Article 14(4) AIA: The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible; (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available; (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system; (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

45 These require that the oversight measures shall be facilitated to users in an accessible and comprehensible way (art. 13(2) and 13(3)(d)).

46 This effort is often absent in other relevant recent EU laws. See Vagelis Papakonstantinou & Paul De Hert, 'Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI' *European Law Blog*, 1 April 2021, 3p. via https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/

47 This is relevant to our analysis, as it will help us to illustrate the two mechanisms in this provision. Nonetheless, it is also relevant to understand how human oversight as a mandatory requirement has been improved for the AIA

48 European Commission (n 34) 21.

all formula. Human oversight is achieved through appropriate mechanisms that require different kinds of human involvement or intervention in the decision-making process, or even in previous design or development stages. In our opening sections we mentioned the GDPR-distinction between *human in the loop*[49] and *human out of the loop*.[50] We intend to analyse more closely this distinction later (sections 5 to 7). Here we learn from the White AI-Paper about the possible variations of human intervention:

Manifestation of human oversight	*Example*	*Governance mechanism*
The output of the AI system does not become effective unless it has been previously reviewed and validated by a human.	The rejection of an application for social security benefits may be taken by a human only	Human in the loop
The output of the AI system becomes immediately effective, but human intervention is ensured afterwards.	The rejection of an application for a credit card may be processed by an AI system, but human review must be possible afterwards	Human out of the loop
Monitoring of the AI system while in operation and the ability to intervene in real-time and deactivate.	A stop button or procedure is available in a driverless car when a human determines that car operation is not safe	Human on the loop Technical feature
In the design phase, by imposing operational constraints on the AI system.	A driverless car shall stop operating in certain conditions of low visibility when sensors may become less reliable or shall maintain a certain distance in any given condition from the preceding vehicle	Technical feature + Human back in control

In a non-exhaustive way, the White Paper lists four different possible human interventions:[51]

- The first example is based on the *human in the loop-governance* mechanism, maintaining a human agent as the final authority over the AI system, which works as a decision support system.[52]
- The *human out of the loop*-mechanism is represented in the second example. The distinction (in the loop/out of the loop) rests on whether the human intervention is ensured before or after the output of the AI system becomes 'effective'. Since the system operates and adopts decisions by default without human intervention, a human out of the loop can be defined as a second-step review of the automated decision.
- The third manifestation shows a variation of the human in the loop-mechanism, known as *the human on the loop*: the role of the human agent is limited to monitoring the system's operation, more like supervision in real-time.[53] But this example also provides a technical feature ('stop button') introduced

49 Human intervention as an essential component of decision-making; see Article 22(1) GDPR decisions.
50 Human intervention as a safeguard on request; see Article 22(2) GDPR decisions.
51 Ibid 21.
52 It should be noted that there are two different conceptions of what the human in the loop actually is. Under a narrow/technical conception, it could be defined as: *'the process when the machine or computer system is unable to solve a problem, needs human intervention like involving in both the training and testing stages of building an algorithm, for creating a continuous feedback loop allowing the algorithm to give every time better results'* Vikram Singh Visen, 'What Is Human in the Loop Machine Learning: Why & How Used in AI?' (*Medium*, 2020) <https://medium.com/vsinghbisen/what-is-human-in-the-loop-machine-learning-why-how-used-in-ai-60c7b44eb2c0>. This conception focuses on the interaction of humans with machines to maintain the human in the algorithmic-loop. Instead, a broader/normative conception focuses on the human intervention to maintain her in the decision and control loop, that generally includes maintaining the human operator as the final authority over the automate system. The latter meaning is adopted in this text. By contrast, a human-out-of-the-loop-system is a fully automated process without any kind of human involvement Aurelia Tamò-Larrieux, 'Decision-Making by Machines: Is the "Law of Everything" Enough?' (2021) 41 Computer Law & Security Review 105541, 13.
53 Joel E Fischer and others, 'In-the-Loop or on-the-Loop? Interactional Arrangements to Support Team Coordination with a Planning Agent' (2017) n/a Concurrency and Computation: Practice and Experience e4082, 1.

in the design and development stages of the AI lifecycle, which is under control of the human on the loop during its use stage.

- A fourth possible mechanism of human oversight in the White Paper is also combined with a technical feature introduced in the design and development stages. In this case, the stop function works without human intervention, and automatically, the AI system decides when to give control over the car to the human agent. We have labelled this mechanism as *human back in control.*

While the White Paper lists different human intervention governance mechanisms mixed with technical features that facilitate human oversight, the Artificial Intelligence Act focuses on mandatory requirements for providers that enable the individuals to whom human oversight is assigned[54] to understand the capacities and limitations of the system, correctly interpret its outputs, or interrupt the system, among others (14(4) AIA), including technical features when possible (13(3)(a) AIA). In our view, the AIA builds on the scheme outlined in the White Paper to consolidate mandatory human oversight for high-risk AI systems. Through different manifestations of human intervention, the White Paper emphasised the idea that human oversight is achieved through appropriate mechanisms that require different kinds of human intervention.

On this basis, the Artificial Intelligence Act goes one step further and establishes new obligations for the design and development of AI systems, without imposing a particular type of intervention at the decision-making stage. This way, it seeks to ensure that human intervention can be effective irrespective of the type of intervention that occurs at the decision-making stage. Users, as data controllers, will acquire AI systems that can be effectively overseen by natural persons, and will therefore affect the way in which they provide the human intervention required by the GDPR in the use of those systems.[55] In our view, what the AIA seems to say is that human intervention by itself is not enough to achieve appropriate human oversight, and therefore, we need further human governance for the design and development stages of AI systems.[56]

5. A closer look into human intervention governance mechanisms in Article 22 GDPR

We saw that Article 29(6) AIA refers explicitly to the DPIA-duties in the GDPR. It is a beautiful example of how the AIA tries to interact and boost the accountability duties contained in the GDPR. According to the EDPB and the EDPS, the important place given to human oversight in the Artificial Intelligence Act is key to ensure that the right not to be subject to a decision based solely on automated processing under the GDPR is respected.[57] Here we have a clear connection of human oversight as a mandatory requirement for AI high-risk systems in the European policy initiatives and human intervention governance mechanisms.

Bearing in mind that the GDPR already includes governance mechanisms based on human intervention in Article 22, we will take a look at them from this perspective. As mentioned in section 2, this provision is grounded on a risk-based approach, which depends on the effect that a decision process can have

54 This is, the human agents introduced in the use stage by the human intervention governance mechanisms.
55 This does not mean, however, that all ADM systems falling within the scope of Article 22 GDPR also would fall under the scope of the Artificial Intelligence Act, but only high-risk AI systems.
56 We will come back to this idea in section 13.
57 EDPB-EDPS, 'Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (2021) 6.

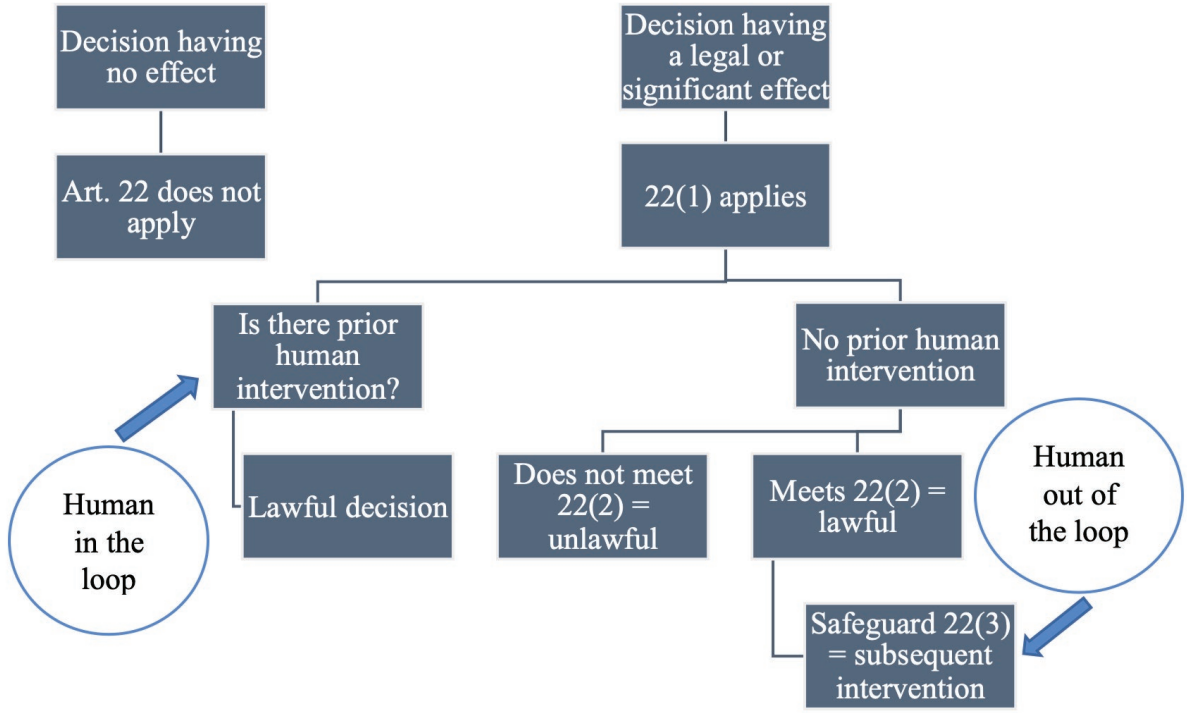
and not only on the degree of automation of the decision process. In the spirit of Article 22 GDPR three possible decisions can be distinguished:

- *no-article 22 decisions*: decisions based –solely or not– on automated processing which don't produce legal effects concerning the data subject or similarly significantly affects him or her;
- *article 22(1) decisions*: decisions that produce legal/similar effects, but are *not* based solely on automated processing (the controller adds a human agent to the decision-making loop)
- *article 22(2) decisions*: decisions that produce such effect, that *are* based solely on automated processing *because* they fall under the 3 exceptions to the prohibition

The first type-decisions are out of the scope of article 22 GDPR, whereas the two other decisions, -'risky' decisions that produce legal or similarly significant effects- are covered by Article 22 GDPR and require mandatory human intervention governance mechanisms. Whenever these effects take place, the Article 22(1) GDPR-prohibition introduces human intervention as an essential component of decision-making: the controller can avoid the prohibition if the decision is not based solely on automated processing, thus introducing a human into the decision loop. For the third type of decisions, -those based solely on automated processing allowed by the 22(2) exceptions-, the GDPR introduces a right/safeguard on request based on human intervention.

But these are two different governance mechanisms that take place at different stages of decision-making. We have outlined above that Commission's White Paper on AI states that human intervention governance mechanisms can take different types and degrees to achieve human oversight. In this regard, we already noted that it makes a clear distinction between the human in the loop and the human out of the loop as governance mechanisms.[58] Let us look more closely at the difference between these mechanisms in Article 22 GDPR.

58 To draw this distinction, it is important to note that for the White Paper the distinction lies on whether the human intervention is ensured before or after the output becomes 'effective', while in the GDPR lies on whether the human intervention is ensured before or after the output 'produces a legal effect concerning the data subject or significantly affects him or her'.



6. Article 22(1) decisions require humans in the loop

The governance mechanism in Article 22's first paragraph closely resembles the first mechanism of intervention listed in the White Paper on AI.[59] Decisions based solely on automated processing are generally prohibited, so any lawful decision that produces a legal or significant effect must incorporate human intervention to the data-processing decision loop.[60] Therefore, any decision that produces such effect must have prior human intervention, a human in the loop.[61] Thus, the general prohibition entails a right to a human in the loop.[62]

Anticipating our discussion of Article 22(2) GDPR-decisions in the next section, we observe that the distinction between human intervention in 22(1) and 22(2) decisions in the GDPR is not just about the stage of decision-making at which the intervention takes place (as we contended in the previous section), but also about the regulatory goal of the intervention itself. The intervention provided by the prohibition shall be the guarantee that the data subjects have the right not to be subjected to fully automated decisions, based solely on automated processing. The GDPR introduces here human intervention as an essential component of decision-making.[63] Then, human intervention is at this point a regulatory remedy to avoid a certain way of processing personal data when it produces risky effects.[64] This way, it is ensured that the decision involves human decision-making as well, and then, the automated systems are not the sole reason for decision-making.[65]

59 See *above*, section 5. *The output of the AI system does not become effective unless it has been previously reviewed and validated by a human (e.g. the rejection of an application for social security benefits may be taken by a human only).*

60 There is only a way to avoid this human intervention or, in other words, to adopt a decision based solely on automated processing: the exceptions regulated in 22(2).

61 Unless it meets one of the exceptions in 22(2) GDPR. In this case, decision-making based solely on automated processing is lawful as long as safeguards contained in the third paragraph are ensured.

62 Jones (n 18) 224.

63 Below we explain in detail that the GDPR requires such human intervention to be meaningful on the part of the controller.

64 The wording of the first sentence in Recital 71 seems to be clear in this sense: *The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.*

65 Ben Wagner, 'Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems' (2019) 11 Policy & Internet 104, 108.

7. Article 22(2) decisions require humans only on request (out of the loop)

Article 22(3) GDPR mandates human intervention by the controller as a safeguard when 22(2)-decisions (= automated decisions with a legal or significant effect made possible by the 3 exceptions) are taken. This is very similar to what is proposed in the White Paper's example of *human intervention on request* discussed *above*.[66] The legal or significant effect occurs prior to human intervention because it is a lawful decision based solely on automated processing, under one of the mentioned exceptions in paragraph 2. But again, it is lawful as long as it is ensured the right to obtain subsequent human intervention, a human out of the decision loop, among other safeguards.

Note that the right to obtain human intervention *a posteriori* is not the *backbone* of the safeguards provided in 22(3) GDPR. A systematic and teleological reading of this paragraph reveals that human intervention is only a minimum requirement to satisfy the main aim of this provision, this is, the right to contest the automated decision.[67] Furthermore, the human out of the loop safeguard is allocated on the basis of contestation by data subjects.[68] From this perspective, the intervention provided by the safeguard aims to re-evaluate a certain way of processing personal data,[69] generally prohibited and only exceptionally allowed.[70]

Whatever the quality of the two governance mechanisms is -in or out of the loop-, it is now time to analyse what kind of human intervention is required: *how much human intervention is needed to satisfy the GDPR?*

8. 'Meaningful' intervention: the WP29 standard accepted in case law but still hard to define

In section 2, we identified some ambiguous phrases in the text of Article 22(1) GDPR that might erode its general prohibition on ADM. An example is the expression 'based solely on automated processing'. The vagueness of 'solely' is far from helpful for a precise understanding of human intervention in 22(1) GDPR-decisions.[71] To understand the term and to make the prohibition work one needs to determine the

66 We recall the second form of human oversight provided by the 2020 White Paper on AI: *The output of the AI system becomes immediately effective, but human intervention is ensured afterwards (e.g. the rejection of an application for a credit card may be processed by an AI system, but human review must be possible afterwards).*

67 See Emre Bayamlıoğlu, 'The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the so-Called "Right to Explanation"' [2021] Regulation & Governance 1; Clément Henin and Daniel Le Métayer, 'A Framework to Contest and Justify Algorithmic Decisions' (2021) 1 AI and Ethics 463.

68 In this regard, Recital 71 GDPR mentions human intervention for a second instance, this time related to the exceptionally allowed processing: *(…) In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.*

69 Almada (n 42) 1.

70 Binns holds that relying on contestation may undermine the equitable application of individual justice: *First, it puts the onus on decision subjects to mount a successful challenge, which may require resources and privileges that are not distributed equally, compounding disadvantage by disproportionately preserving individual justice for those who are already advantaged. Second, it means that decision-makers are likely to only review false positives (where people have been incorrectly denied a benefit) and ignore false negatives (where people have incorrectly been granted a benefit), because the latter have no incentive to challenge a positive decision*, see Reuben Binns, 'Human Judgment in Algorithmic Loops: Individual Justice and Automated Decision-Making' [2020] Regulation & Governance 11. Binns' second argument teaches us that human intervention on request-mechanism in Article 22(3) GDPR is not the best or most optimal GDPR-option from a human rights perspective. First, because it is allocated on the basis of contestation and, secondly, because it is instrumental to the right to contest the decision based solely on automated processing.

71 Elena Gil González and Paul de Hert, 'Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles' (2019) 19 ERA Forum 597, 617.

threshold of minimum human intervention required not to make a decision-making 'solely automated'. If the legal world allows a mere light-touch intervention to qualify as human intervention the whole protective mechanism of Article 22 GDPR falls flat on its face.

Some authors, referring to German case law, seem to believe that a light-touch human intervention would survive judicial review.[72] In our view, it is clear that being satisfied with any minimal human intervention contradicts existing soft law guidance on Article 22 GDPR as contained in the Article 29 Working Party's Guidelines on Automated individual decision-making, a document that was endorsed by the EDPB.[73] Central in this document is the requirement that human intervention needs to be *meaningful*.[74] The central message of these guidelines seem to have been picked up in more recent case law.[75]

The WP29-*Guidelines* are an impressive document of 37 pages and 6 sections (with only one section devoted to Article 22 GDPR). The document starts with defining both profiling and automated decision-making,[76] and organizes the landscape by distinguishing between automated decision-making based on profiling that is not covered by Article 22 GDPR; and solely automated decision-making, including profiling covered by Article 22 GDPR. An example of the former category is *before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful intervention carried out by humans before any decision is applied to an individual*.[77]

72 One of the main critiques to this provision states that mere nominal human intervention is often included in the decision-making process to exclude the applicability of the information rights for automated decision-making contained in articles 13(2)(f), 14(2)(g) and 15(1)(h), and therefore, also to avoid the need to comply with the exceptions contained in 22(2) and safeguards in 22(3). See Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76, 88. However, this critique by Wachter, Mittelstadt and Floridi is based on the German Federal Court's interpretation of Article 15 Directive 95/46/EC concerning the SCHUFA credit reports (Judgment of the German Federal Court: Scoring und Datenschutz BGH, 28. 1. 2014-VI ZR 156/13). One can open a discussion about the relevance of this German case. Contrary to this position, Brkan states that *a formalistic interpretation, involving the human only as a necessary part of procedure but ultimately leaving the decision power to the machine, would not ensure a sufficiently high level of data protection of the data subject*, Brkan (n 17) 101.

73 Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018).

74 Indeed, according to the interpretation endorsed by the EDPB, the first paragraph of the Kafkaesque provision requires human intervention to be meaningful. This reasoning is developed throughout the above-mentioned guidelines.

75 Recently, the Amsterdam District Court interpreted Article 22 GDPR according to these guidelines: *A decision based solely on automated processing exists if there is no meaningful human intervention in the decision-making process*. See paragraph 4.63. *Uber transparency request* case (C/13/687315 / HA RK 20-207), paragraph 4.37. *Ola transparency request* case (C/13/689705 / HA RK 20-258) and paragraph 4.10. U*ber deactivation* case (C/13/692003 / HA RK 20-302) [*Van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit is sprake indien er geen betekenisvolle menselijke tussenkomst is in het besluitvormingsproces].*

76 'Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar. The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person. A simple classification of individual ls based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusion about an individua l. In this case, the purpose is not assessing individual characteristics and is therefore not profiling'. Both profiling and ADM can be risky in terms of fundamental rights. Not all forms of classification of individuals amounts to profiling, what is needed is some form of evaluation or assessment or judgement. There can be profiling without automated decision-making (and vice versa). Profiling in the sense of the GDPR requires some automated processing, but not necessarily solely automated processing. Comp. 'Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition', see Article 29 Data Protection Working Party (n 73) 7.

77 ibid 8.

It is interesting to see how the criterium of 'meaningful' finds its way in this example as a key notion to determine *when something is not Article 22(1) GDPR* or 'not solely automated processing'. This kind of processing is related to a meaningful –not any minimum– human intervention.[78]

The criterion of meaningful returns in the *Guidelines* towards the end where the question is addressed what qualifies as human involvement that prevents decisions based solely on automated processing in the light of the controllers GDPR duties. The controller cannot avoid the Article 22(1) GDPR-prohibition by fabricating human involvement, writes the Working Party 29. Therefore, controllers must ensure that any human intervention is *meaningful* to the decision-making process for 22(1) decisions.[79] The same must be said on the human intervention that needs to be provided as a safeguard on request for fully automated 22(2) decisions.[80]

It is true, the *Guidelines* acknowledge, that controllers can avoid the information rights and safeguards that are mandatory for 22(2) decisions by including a human agent in the loop.[81] However, this does not mean that the GDPR provides a wild card to fabricate human intervention either.[82] As it is explained in the Guidelines controllers need to *significantly* increase the level of human intervention to avoid the 22(1) GDPR-prohibition.[83]

Hence, the *Guidelines* are unambiguous: the kind of intervention required under Article 22 GDPR is therefore *meaningful*.[84] But does this solve all disputes or is this just lifting the discussion to another level of vagueness? Determining what could be meant precisely by meaningful[85] is indeed an even more complicated -but necessary- task. The scarce precedents in the CJUE and national courts do not make it any easier. One approach for the interpretation of this term can be found in the *Guidelines*. They provide some elements to understand both human intervention as an essential component and as a safeguard

78 Again, to draw the difference between decision-making based on profiling and solely automated decision-making, the Article 29 Working Party states that the latter is delivered to the individual, *without any prior and meaningful assessment by a human*, ibid 9. Consistent with our previous analysis, human intervention needs to take place prior to the effects defined by the provision.

79 ibid 21. This is also stated by the Spanish DPA in its guidelines on the adequacy of processing involving Artificial Intelligence with regard to the GDPR: *In order to be considered human involvement, the supervision of the decision must be carried out by a person authorised and competent to modify the decision, and must be meaningful and not a token action* [*Para que pueda considerarse que existe participación humana, la supervisión de la decisión ha de ser realizada por una persona competente y autorizada para modificar la decisión, y para ello ha de realizar una acción significativa y no simbólica*] AEPD, 'Adecuación Al RGPD de Tratamientos Que Incorporan Inteligencia Artificial. Una Introducción' (2020) 10. Also, the UK's Information Commissioner's Office states in its guidance on automated decision-making and profiling that the human involvement has to be active and not just a token gesture: *The question is whether a human reviews the decision before it is applied and has discretion to alter it, or whether they are simply applying the decision taken by the automated system*, ICO, 'Guide to the UK General Data Protection Regulation (UK GDPR)' (2020).

80 Article 29 Data Protection Working Party (n 73) 27.

81 It should not be forgotten, nevertheless, that the general GDPR rules and standards will apply to profiling even when a human in the loop plays a meaningful role in the creation of the relevant profile. Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' (2018) 9 JIPITEC 55.

82 In this sense, the introduction of human intervention as a governance mechanism does not weaken the data protection framework. It does, however, reveal one of the weaknesses of the GDPR that has been pointed out in the literature: an insufficient protection of the outputs generated by automated data processing. Indeed, Wachter and Mittelstadt highlighted that the majority of the mechanisms in the GDPR focus on management of input data, see Sandra Wachter and Brent Mittelstadt, 'A Right to Resonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] Colum. Bus. L. Rev. 1.

83 Article 29 Data Protection Working Party (n 73) 30.

84 Nevertheless, we believe that this element should have been explicitly included in paragraphs 1 and 3. The term 'solely' could be rewritten as 'based on automated processing without meaningful human intervention'. And the safeguard on request in paragraph 3 could provide a 'right to obtain meaningful human intervention'. Similarly, Noto La Diega states: *Therefore, it would seem more appropriate to recognise the right not to be subject to an algorithmic decision every time that there is not a human being clearly taking the final decisio*n, Noto La Diega (n 81) 54.

85 Neither it is explained what is meaningful related to information rights in articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR, even if the term was included explicitly. Ida Koivisto, 'Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-Making' (2020) 2020/01 Academy of European Law working papers 1, 17.

on request.[86] The intervention should be carried out by someone who has the authority and competence to change the decision,[87] and the analysis of the outcome should consider all the relevant data.[88] The only difference we find considering the human in the loop and the human out of the loop on request in the GDPR is that the latter should include any additional information provided by the data subject.[89]

At this point, it seems obvious that further legal work is necessary on this concept. It is clear that Article 22 GDPR deserves to be complemented and that 'meaningful' should be part of the new rewritten GDPR.[90] For a start, since Article 29 Working Party's guidelines clearly stated that required human intervention under the GDPR shall be meaningful, the European Data Protection Board could contribute with new guidelines clarifying this concept.[91]

9. Humans safeguard against loss of control by citizen over decisions affecting them (contestability at stake)

A further approach to fleshing out the meaningfulness of human intervention governance mechanisms is to dig into the rationale behind these GDPR-provisions (teleological interpretation). The preparatory works of the GDPR, more focused on profiling and its discriminatory effects, shed however little light on Article 22 GDPR's rationale.[92] We do find some clues in the preparatory works with regard to Article 15 of Directive 95/46/EC, that is said to express fear for the future of human dignity in the face of machine determinism.[93] In the preparatory works of this Directive the Commission also pays attention to the dangers of the objective and incontrovertible character of sophisticated software, *to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities*.[94]

So, human intervention is a response to this notion of abdication of human responsibilities and its consequences for the data controllers (relying on machine's outputs and loss of quality in decision-making) and for data subjects (machine determinism causing loss of human autonomy and dignity).[95]

In our view, these fears about abdication through reliance on automatic decision-making need to be looked at from the perspective of data controllers and of data subjects.

86 Article 29 Data Protection Working Party (n 73) 21 and 27.

87 Recital 48 of the Artificial Intelligence Act considers that the natural persons to whom human oversight have been assigned shall have *the necessary competence, training and authority to carry out that role.* Nevertheless, no obligations on users of high-risk AI systems with this content are included in the article 29.

88 Considering all the relevant data by the human agent might present enormous difficulties in practice: *In particular, it remains unclear how a human with limited capacities of data analysis will be able to justify that the final decision needs to be different from an algorithmic one, given that the automated system might not only have taken into account the data relating to the data subject affected by the decision, but a multitude of other complex datasets. If the automated decision was a simple sum of data appertaining to a particular data subject, an in-depth human review of automated decision would be much more feasible. If, however, the decision is based on complex relations between data in a Big Data environment, the human will have a much more difficult task in reviewing such a decision.* Brkan (n 17) 108.

89 Article 29 Data Protection Working Party (n 73) 27.Which reaffirms the link of human intervention as a safeguard to data subject's rights to express his or her point of view and to contest the decision, see Almada (n 42) 1; Malgieri (n 16) 22.

90 Hert and Lazcoz (n 17).

91 Almada highlights the relevance of identifying whether human intervention in the decision-making process is meaningful or merely nominal: *In a scenario where the lines between full and partial automation are blurred, individuals might find themselves uncertain of the adequate channels for recourse, and this lack of information may cause delays or even block the reparation of harms caused by automation.* Also notes that drawing this difference in practice might be challenging, Marco Almada, 'Automated Decision-Making as a Data Protection Issue' (2021) 7 Available at SSRN: https://ssrn.com/abstract=3817472.

92 Mendoza and Bygrave (n 24) 83.

93 Lee A Bygrave, 'Minding the Machine: Art 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Review 18.

94 European Commission, 'Amended Proposal 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 (COM(92) 422 Final)' (1992) 26.

95 Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling BT - EU Internet Law: Regulation and Enforcement' in Tatiana-Eleni Synodinou and others (eds) (Springer International Publishing 2017) 84.

From the perspective of data subjects these fears for machine determinism circle around the concept of contestability. We are in the hypothesis of Joseph K. in Kafka's novel, who had to deal with an unreasoning and unreasonable authority that imprisoned him. What is at play here not about fear about humans letting machines make bad choices (as discussed in the next section) but a concern to uphold human dignity by ensuring that humans (and not their 'data shadows') maintain the primary role in 'constituting' themselves. Mendoza and Bygrave rightly observed that the primary catalyst for Article 15 of the Directive was 'the potential weakening of the ability of persons to exercise influence over decision-making processes that significantly affect them, in light of the growth of automated profiling practices'.[96]

This ambition transcends the mere objective of transparency or creating a human contact for the data subject, it aims some sort of control by data subjects. Nevertheless, control as a rationale in the GDPR does not imply absolute control of individuals over their personal data, but rather the ability to participate in and influence the data processing.[97] Human intervention governance mechanisms as contained in Article 22(3) GDPR 'use' transparency as a means to provide data subjects with the possibility to exercise other rights recognised in the GDPR[98] and influence over the decision-making process.[99] The dignity resides in the action of exercising influence: human intervention on the side of the data controller is a precondition for human control on the side of the data subject.[100]

Therefore, the introduction of human intervention as a safeguard on request for Article 22(2)-decisions is connected to data subject's rights to express his or her point of view and to contest the decision.[101]

96 ibid 83. As they show, this perspective was also explicit in the preparatory works for Directive 95/46/EC: *This provision is designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. 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'.* European Commission, 'Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security (COM(90) 314 Final)' (1990) 29.

97 Mariam Hawath, 'Regulating Automated Decision-Making: An Analysis of Control over Processing and Additional Safeguards in Article 22 of the GDPR.' (2021) 7 European Data Protection Law Review 161, 162–163.

98 Roig (n 26) 47.

99 Nonetheless, the GDPR lacks any connection between 22(1) decisions and the exercise of information rights under the transparency principle. Quite the contrary, we have already pointed out that the introduction of a human in the loop avoids the exercise of the rights contained in articles 13(2)(f), 14(2)(g) and 15(1)(h).

100 The French *Conseil Constitutionnel* (Conseil Constitutionnel, Décision n° 2018-765 DC du 12 juin 2018, §71) declares human intervention a fundamental safeguard in the design and development of AI algorithms, see Malgieri (n 16) 15. And further recognises the link between this safeguard and the ability to explain, in detail and in an intelligible form, how the processing has been carried out to data subjects. In this regard, the human agent might be an intermediary providing a dynamic explanation, particularly in cases where satisfactory explanations are not easy to reach a human-mediated explanation might be helpful, see Ronan Hamon and others, 'Impossible Explanations? Beyond Explainable AI in the GDPR from a COVID-19 Use Case Scenario', *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2021) 558. On human intervention as a mediation between black-box algorithms and explanations, Robbins and Henschke hold that: *The solution, therefore, is to use such algorithms for specific situations in which it is acceptable to not have an explanation or to supplement the decision of the algorithm with human oversight. Placing someone on the No-Fly list, for example should not be solely decided on the basis of an algorithm which can offer no explanation. A restriction of one's rights is a moral decision and only a human being can accept the moral responsibility which comes along with such a decision.* Stephanie A Robbins and Adam Henschke, 'Designing for Democracy : Bulk Data and Authoritarianism' (2017) 15 Surveillance and society 582, 588. Nonetheless, this link should be managed carefully, as Koivisto warns: *The more human mediation there is, resulting in carefully managed visibilities, the more legitimacy may be produced. At the same time, this may also mean less "truth", when the intricacies of the black box cannot, by being exposed, necessarily communicate anything (the truth-legitimacy trade-off)* Koivisto (n 85) 19.

101 This seemed to be the same perspective as that held by the Council of Europe in its Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. In this document, the role of humans in decisions based on Big Data is to upon request of the data subject, provide her or him with the reasoning underlying the processing, and to not rely on the automated decision on the basis of reasonable arguments. This was later reflected in Article 9(1)(a) of the COE Convention 108+, as a right 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.*

Equally, human intervention as a governance mechanism in Article 22(3) is aimed to request a second-step decision, in which a human agent can take into account also the point of view of the data subject.[102] Which is reaffirmed by Article 29 Working Party's Guidelines, when they clarify that human intervention as a safeguard on request should include any additional information provided by the data subject, which is not stated for human intervention in 22(1) decisions.[103] This connection reveals how both rights to obtain human intervention and to express her point of view are instrumental to the *backbone* in 22(3) safeguards: the right to contest the decision.[104]

Therefore, humans can be introduced by regulators to facilitate contestability for those who are affected by the automated decisions. In the GDPR this rationale for making humans intervene is found as a safeguard on request for decisions based solely on automated processing. However, this ground for involving humans in ADM will always be instrumental to the right to contest the decision. In other words, human intervention is there as an individual right to protect the subjective interests of data subjects. And this approach has severe limitations in the ADM context.[105] In our view, there is a second rationale for human intervention that is usually forgotten and deserves our attention.

10. Humans safeguard against loss of control by controllers over their decisions (accountability at stake)

Let us continue our teleological interpretation (that is, understanding the rationale) of Article 22 GDPR by looking at the fears about abdication of human responsibilities from the perspective of data controllers. This is, at what happens when data controllers attach *too much weight* on ADM.

Of course, this abdication is unacceptable from a data protection law perspective. The problem here is not contestability, but accountability. Article 22 GDPR reflects European scepticism towards biases and potentially false decisions that can be taken by machines not verified by humans.[106] Uncontrolled processing activities are disrespectful of major data protection principles, such as fairness (and non-discrimination) and accuracy. [107] Humans are crucial to avoid improper correlations and thus to ensure

102 In this regard, Malgieri (n 16); also Almada (n 42). Again, Koivisto notes that it should not be forgotten that the exercise of transparency rights requires in any case human involvement that is relevant for the legal analysis, whether we talk about transparency or the right to explanation, or meaningful information about the logic involved. Koivisto (n 85) 19.

103 Article 29 Data Protection Working Party (n 73) 27.

104 In Bayamlıoğlu's own words: *It obliges the data controller either to render automated decisions contestable or to cease ADM at all. What is required by Article 22(3) is not about informing or disclosing but rendering the decision contestable at least against a human arbiter.* Bayamlıoğlu (n 67) 5.

105 It is based on presumptions such as that the protection of individual interests prevails over other interests of a general nature in this kind of data processing. Or that individuals are sufficiently empowered to contest this kind of processing effectively. This does not correspond to the evidence. See Bart van der Sloot and Sascha van Schendel, 'Procedural Law for the Data-Driven Society' (2021) 30 Information & Communications Technology Law 304.

106 Brkan (n 17) 97.

107 The GDPR states that processing of personal data is subjected to both fairness 5(1)(a) and accuracy 5(1)(d) principles and makes controllers responsible for that. Recital 71 constitutes an explicit requirement for controllers using profiling to minimise the risk of errors in both terms of inaccuracies and discriminatory, and it establishes a explicit link between fairness and non-discrimination in the GDPR, see Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65, 92; Tamò-Larrieux (n 52) 8. Article 29 Working Party highlights that controllers should consider accuracy at all stages of profiling, including building profiles for individuals or applying them to make decisions affecting individuals, Article 29 Data Protection Working Party (n 73) 12. This broad interpretation of accuracy focuses less on the data input but on the output and the overall proper and adequate functioning of an ADM system, again Tamò-Larrieux (n 52) 8; see also Wachter and Mittelstadt (n 82) 615 et seq.

fairness in data mining,[108] and not only to exclude discrimination but also to reduce false positives.[109] In the Commission's view, human oversight helps to ensure that an AI system does not cause adverse effects.[110] Likewise, the Artificial Intelligence Act states that human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights (14(2) AIA).[111]

In this light, human intervention in the GDPR would help to hold controllers responsible for their own decisions and forces them oversee that personal data are processed accurately, fairly and lawfully.[112]

In our view, lack of meaningful human intervention and abdicating one's responsibilities is inescapably linked to the principle of accountability introduced by the GDPR.[113] Making humans intervene at different stages of ADM is a measure aimed at achieving appropriate human oversight of the system *and* appropriate human oversight contributes to hold controllers accountable. Accountability's core idea is to have an accountable person, one that takes control or dominium (control of the processing) and does not abdicate his or her responsibilities, and is moreover capable of proving this dominium via a variety of tools (document holding, impact assessments, security policies, etc.). The principle enshrined in Article 5(2) GDPR is in our view the most pertinent GDPR principle since it is tied intimately to all 6 other GDPR principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality).[114] Accountability commands that controllers take responsibility for what they do with personal data, for compliance with all other GDPR principles and for demonstrate this compliance.

To live up to the principle of accountability necessitates a comprehensive governance structure and a lot of restructuring and paperwork, in the sense that technical and organisational measures need to be implemented and documented.[115] Indeed, Article 24 GDPR calls for the controller's responsibility for the implementation of appropriate technical and organisational measures to ensure and to be able to

108 Maddalena Favaretto, Eva De Clercq and Bernice Simone Elger, 'Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review' (2019) 6 Journal of Big Data 12, 21.

109 Antoni Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' (2017) 8 European Journal of Law and Technology 6. These approaches will be critically addressed in section 13.

110 European Commission (n 34) 21.

111 It is important to note that an accurate output may compromise fundamental rights and thus be unfair or even unlawful. An interesting and debatable idea that this second paragraph in article 14 AIA adds is that human oversight shall aim at preventing and minimising such risks, in particular when they *persist notwithstanding the application of other requirements set out in this Chapter* (such as data quality, transparency or robustness). It is questionable that human intervention can compensate the deficiencies of flawed machines, see section 13.

112 Hence, human intervention will be meaningful when the controller is able to demonstrate that the individuals to whom human oversight is assigned contribute to lawful, fair and accurate data processing.

113 Accountability as a principle is composed by two elements: (i) the need for a controller to take appropriate and effective measures to implement data protection principles; (ii) the need to demonstrate upon request that appropriate and effective measures have been taken. Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 9. See on the principle, Paul De Hert and Dimitra Stefanatou, 'The Accountability Culture in Its European Union Dress. Sticks but No Carrots to Make the Proposed Data Protection Regulation Work' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *En un nuevo régimen europeo de protección de datos. Towards a new European Data Protection Regime* (Tirant lo Blanch 2015); Paul De Hert, 'From the Principle of Accountability to System Responsibility – Key Concepts in Data Protection Law and Human Rights Law Discussions' in Ferenc Zombor (ed), *International Data Protection Conference 2011* (Hungarian Official Journal Publisher 2011).

114 This is evidenced by the structure of Article 5 GDPR enumerating in a first paragraph all six GDPR principles and adding the accountability principle in a second paragraph in these terms: '*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1*'.

115 Among others, Documented processes/policies, records of processing activities, internal guidelines for employees, incorporate training and awareness programs for everyone who is going to be involved in the processing of personal data, data protection impact assessments (DPIA), data security methods, data protection by design and by default, a mandatory data protection officer (DPO) for large scale personal data processing, data breach notification policies and transparency requirements. See Sebastian le Cat, 'GDPR Top Ten #2: Accountability principle. What do organisations need to do to show accountability for their data processing activities?', via https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html

demonstrate that the data processing is performed in accordance with the GDPR. Depending on the risk of the processing, such technical and organisational measures may be imposed by the GDPR. In other cases, the GDPR provides several measures that may be taken by the controller where it considers that they are appropriate. Where data processing is to be used by the controller for ADM purposes with legal or meaningful effects, the GDPR imposes the inclusion of humans -in or out of the loop- as an organisational measure (see sections 5-7). However, the GDPR gives considerable discretion to the controller to decide what kind of ADM system suits her best.[116] This way, human intervention in the GDPR is part of an active knowledge creation process required by the accountability principle.

It is now clear that governance mechanisms for ADM like humans in the loop -22(1) GDPR- or on request -22(3) GDPR- need to be part of a culture of accountable organisations. Below we will argue the role of DPIAs in getting that culture right. The GDPR makes humans intervene in ADM to help organisations to be accountable. Therefore, organisations must in turn be able to demonstrate how these humans contribute to compliance.

11. The role of DPIAs in getting accountable meaningful human intervention set up

In the previous sections, we have explained how human intervention is introduced in Article 22 GDPR and we have linked the rationale of human intervention with the accountability principle. Now, we will analyse whether Article 22 governance mechanisms based on human intervention combine with the GDPR's systemic governance regime.[117]

As we have argued in the previous section, human intervention is introduced in the GDPR as an organisational measure to control risks in data processing. In this regard, we identified Article 22 GDPR and its human intervention mechanisms as a testament to the principle of accountability, a principle that pervades the whole GDPR and demands for comprehensive governance structure based on training, documentation, and organizational and technical measures. Data protection impact assessments (DPIA),[118] mandated by Article 35 GDPR, are a part of this structure and we promised to get back to them, since they can be specifically used to require from controllers to demonstrate compliance with their human intervention duties. We see this accountability tool as an essential pre-requisite for 22(1) and 22(2) compliant decisions.[119]

116 Back to the example provided by the WP29 Guidelines: The controller can still envisage a 'model' of decision-making based on profiling, by significantly increasing the level of human intervention so that the model is no longer a fully automated decision making process. Article 29 Data Protection Working Party (n 73) 30.

117 When it comes to algorithmic accountability, Kaminski and Malgieri argue that the GDPR combines a series of individual rights with a systemic governance regime overseen by the regulators, see Margot E Kaminski and Gianclaudio Malgieri, 'Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations' (2021) 11 International Data Privacy Law 125, 127.

118 DPIA is a process for building and demonstrating compliance. See David Wright and Paul De Hert (Eds.), *Privacy Impact Assessment* (Springer, Dordrecht 2012).

119 Veale and Edwards already suggested that DPIA is adequate to assess what decisions are based 'solely' on automated processing, see Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling' (2018) 34 Computer Law & Security Review 398, 401. Hawath holds that DPIAs, along with Article 5 GDPR principles, can be interpreted to remedy gaps in protection left by Article 22's focus on individual control over ADM. Hawath (n 97) 173.

Firstly, because of the scope of application of DPIAs. Article 35 GDPR is broadly formulated and many ADM systems, whether based solely on automated processing or not, will need to adopt a DPIA.[120] The provision is long and based on a risk-approach,[121] which could leave some to believe that AMD systems are not always subject to the provision. Article 35(3)(a) is however crystal clear by requiring a DPIA in all cases of *systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*.[122]

Article 35 GDPR is equally clear on the specific duties for controllers when carrying out DPIAs. The GDPR requires to define the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects (35(7)(d) GDPR). The rights contained in Article 22 GDPR are no exception among such rights. DPIAs therefore need to define the measures taken by the controller to demonstrate that data subjects are not subjected to unlawful automated decision-making. Or those taken as safeguard measures for decisions based solely on automated processing. Thus, as part of the DPIA, the controller should identify and record the degree of any human involvement in the decision-making process and at what stage this takes place.[123] The assessment needs at least to identify the relevant paragraph in Article 22 GDPR: not fully automated decisions with human intervention prior to the production of the effect should be the rule (Article 22(1)-decisions),[124] and fully automated decisions with *a posteriori* human intervention (Article 22(2)-decisions) should be the exception. We repeat that there are different ways to introduce human intervention into decision-making.[125]

120 Roig (n 26) 113.The provision does not distinguish between fully automated systems and decision support systems. Article 35(3)(a) dismisses the term 'solely', and states that DPIA is mandatory to 'systematic and extensive evaluation of personal aspects (…) *based on automated processing*' This interpretation is also endorsed by the Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017). Also in the Guidelines on ADM, the Article 29 Working Party states that, even if the controllers significantly increase human intervention for the ADM system to avoid the prohibition in 22(1), such system could still present risks to individuals' fundamental rights and freedoms. Article 29 Data Protection Working Party (n 73) 30.

121 Comp. Article 35(1): 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.'

122 The duty to carry out a DPIA before starting a ADM activity cannot be bypassed or mitigated simply by configuring these systems as recommender systems for human decision-makers rather than fully automated systems, see Yeung (n 8) 516. Unlike information rights – 13(2)(f), 14(2)(g) and 15(1)(h) – and safeguards for fully automated decision-making – 22(3) –, which has been criticized Veale and Edwards (n 119) 400. Article 35 applies both to decisions made with and without meaningful human involvement. In passing we note that we agree with Veale and Edwards' criticisms in that information rights should apply both to decisions made with and without meaningful human involvement.

123 Article 29 Data Protection Working Party (n 73) 21.This interpretation is in line with the Commission's White Paper and Artificial Intelligence Act, which consider that the appropriate type and degree of human oversight may vary from one case to another, as explained in sections 4 and 5.

124 What is relevant in light of Article 22(1) is whether the intervention is prior to the production of a significant effect and whether it is meaningful. In other words, to demonstrate compliance with data subjects' right not to be subjected to a decision based solely on automated processing, DPIAs should show that human involvement is meaningful and prior to the production of a significant effect.

125 Even within one legal regime (either the one in Article 22(1) or the one in Article 22(2)) variations and adaptations of human involvement are possible, with or without technical measures. Again, the lack of precedents and legal doctrine on this point hinders the compliance of controllers with such duties. The four examples of human intervention in the 2020 White Paper on AI (discussed in section 4) can serve as a source of inspiration for the controller. Data protection authorities will have a key role in triggering engineers and AI-system producers to develop novel methods (organizational or technical) to make intervention by humans possible.

On the meaningfulness of the intervention, the justificatory explanations demanded by accountability in the GDPR will allow the controller to answer relevant questions such as whether and how the decision-making procedure involves human discretion, how the automated and human elements interact in this procedure, or how this interaction effects aggregate outcomes.[126]

12. DPIAs have limitations, but also room for improvement

Article 35 GDPR is not a brutal game changer. It mentions public participation the DPIA process without making it a hard rule.[127] It equally softly insists on the necessity to incorporate DPIA's in a cyclic process.[128] Essential to understand the nature of the assessment exercise is paragraph 7 of the provision that demands a full description of the envisaged processing activity, its proportionality and necessity, its risks and the measures envisaged to address these risks.[129] Regarding the assessment of human intervention, the description of the authority and competence requirements have a more static formal-institutional character, but the assessment of the other requirements requires continuity over time.[130]

Given that individuals may provide an erratic and uncertain safeguard, an alternative institutional check could prove wise.[131] DPIAs can provide a continuous evaluation of human intervention that enables the controller to demonstrate that the human intervention is meaningful in compliance with the regulatory mandate of the GDPR. When it comes to demonstrating whether human intervention is meaningful or not, there is little room to hold that such meaningfulness can be understood as relating to an individual decision, by looking at whether the human agent has altered an individual decision or not.[132] There is no way to know if a human agent is affected by automation bias evaluating a single decision. This institutional assessment on human intervention allows evaluating the cost-and-incentive structure of the decision-making process.[133] Furthermore, not looking at individual cases but at the larger behaviour of

126 Talia B Gillis and Joshua Simons, 'Explanation < Justification: GDPR and the Perils of Privacy' [2019] Journal of Law and Innovation 71, 95.

127 Article 35(9) GDPR: 'Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations'. See Maria Eduarda Gonçalves, 'The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward' (2017) 26 Information & Communications Technology Law 90.

128 Article 35(11) GDPR: 'Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations'.

129 Article 35(7) GDPR: 'The assessment shall contain at least: 1) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; 2) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; 3) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and 4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned'.

130 This is consistent with the nature of the DPIA itself. According to data protection by design and by default principles, the DPIA needs to be carried out prior to the processing. Nonetheless, it has to be updated throughout the system's lifecycle, since it is conceived by the GDPR as a continual process, rather than as a one-time exercise, see Article 29 Data Protection Working Party (n 120) 14.

131 Huq (n 28) 682.

132 Here, we disagree with Noto La Diega. He states that whether human intervention is meaningful might only be assessed on a case-by-case basis and, therefore, the application of 22(1) decisions should also depend on that case-by-case basis, see Noto La Diega (n 81). Our view is quite the opposite.

133 For instance, the human agent may be influenced by the institutional cost and incentive structure to follow or deviate from automated decisions based on criteria that do not respond to more accurate or fairer decision-making. In this sense, Sartor and Lagioia warn: *Moreover, human intervention may be prevented by the costs-and-incentives structure in place: humans are likely not to substantially review automated decision, when the cost of engaging in the review – from an individual or an institutional perspective– exceeds the significance of the decision (according to the decision-maker's perspective).* Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence (PE 641.530)' (2020) 60.

ADM systems through DPIAs can help data controllers to prevent societal side-effects of those systems that extend beyond the individual level[134] and, therefore, check how human intervention can influence in the mitigation of such effects.

However, meaningful human intervention is not a panacea-solution, neither impact assessment tools are. DPIAs in the GDPR are mainly self-assessment governance tools -combined with the potential control of the Supervisory Authorities-,[135] and its core value rests on leading to the building of better systems overall.[136] Carrying out DPIAs, data controllers should be aware of human intervention's role in the overall. If the GDPR confers a key role to DPIAs in mitigating the discriminatory effects of data processing,[137] we understand that it is essential to assess how human intervention contributes to this purpose. In other words, the assessment of meaningful human intervention is one of the procedures that impact assessments put in place, which can serve *not just to prevent error, bias, and discrimination, but also to legitimize a system or even respect an individual's dignity within it*.[138]

A new development, with the potential to boost the duty to carry out impact assessments, might be expected to come from the adoption of the forthcoming EU law(s) on AI. Risk-impact assessment tools will have a determinant role for the compliance with mandatory requirements for the development and use of high-risk AI-systems.[139] Following on from the discussion in section 3 above, under the AIA users (controllers) of high-risk AI systems shall make use of the information given by the providers of AI systems under the transparency requirement *to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 (…), where applicable* (29(6) AIA). This information includes human oversight measures (13(3)(d) AIA). In other words, users (controllers) will receive technical and organizational information (from the AI system-providers) about the AI systems they acquire and are obliged to make use of this information that enable the individuals (in the controller's organisation) to whom human oversight is assigned in Article 22 GDPR to understand the capacities and limitations of the system– to comply with Article 35 GDPR. This new layer of mechanisms and tools complements the GDPR-governance system in a promising way that benefits not only GDPR-data subjects but also GDPR-controllers, since the AIA proposal will broaden their possibilities to provide and demonstrate meaningful human intervention as data controllers in the GDPR.

To summarise, Article 35 GDPR requires controllers to continuously demonstrate how human intervention is introduced to comply with data subject's right not to be subject to automated individual decision-making. This does not mean that the regulation imposes a specific model of human intervention, nor does it mean that it should be understood apart from the rest of the measures and safeguards to demonstrate compliance with the GDPR.

134 Tamò-Larrieux (n 52) 14–15.
135 Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754, 768; Hawath (n 97) 171.
136 L Edwards and M Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16 IEEE Security & Privacy 46, 51.
137 Roig (n 26) 114.
138 Kaminski and Malgieri (n 117) 140.
139 Although in this text we focus on DPIAs, it is possible that future regulation will incorporate impact assessment tools with a broader scope of application, such as the human rights impact assessment (HRIA) model proposed by Mantelero and Esposito, see Alessandro Mantelero and Maria Samantha Esposito, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review 105561.

13. What should data controllers do when human intervention is meaningless?

The scenario is the following: while carrying out a DPIA, controllers may find out that human intervention is meaningless in the decision-making process. This is, they introduce human agents that intervene in the decision-making process prior to the production of any legal or significant effect to the data subjects. Nonetheless, the assessment of the intervention[140] shows either that it does not contribute to more fair or accurate decisions, or that humans are routinely applicating the algorithmic outputs, therefore, suffering automation bias.

In this case, taking into account the above-mentioned wide spectrum to comply with 22(1) GDPR, controllers should consider implementing different human-machine decision-making models.[141] Indeed, machines are outperforming humans in more and more tasks, but this does not mean that human intervention cannot be meaningful at all. As noted before, both the White Paper and the Artificial Intelligence Act consider that the appropriate type and degree of human oversight may vary from one system to another. Likewise, the GDPR does not impose a particular type and degree of human intervention, as long as it is meaningful and prior to the production of the effects described in Article 22(1).[142] Then, controllers are given a wide spectrum of ways to comply with human intervention as an essential component of decision-making imposed by the Regulation.

Evidence shows how well-designed interactions between human intelligence, machine intelligence, and organisational measures can mitigate discriminatory effects[143] and improve decision performance.[144] Binns holds that there is a model of collaboration between humans and machines arguably implied in Article 22(1): *in which human reviewers attend to the individual circumstances of the case; meanwhile, algorithms take care of inducing patterns across multiple cases to predict outputs*.[145] In our view, the DPIA is an adequate tool to evaluate –and re-evaluate if necessary– the best possible model of collaboration under 22(1) GDPR.[146] Finally, where human intervention in the loop is not meaningful and no remedy is possible, data subjects will be subjected to decisions based solely on automated processing. This means that, unless an exception 22(2) is met, such data processing is prohibited.

140 As mentioned above, consistent with data protection by design and by default principles, the DPIA should be carried out prior to the processing. Therefore, this assessment needs to take place at that stage. However, since the DPIA has to be updated throughout the system's lifecycle, this scenario could arise at any point of the lifecycle.

141 The Commission's response in the White Paper seems straightforward, if it does not work, try to remedy it: *In case the conformity assessment shows that an AI system does not meet the requirements (…), the identified shortcomings will need to be remedied* (WP, p.23).

142 Neither the Courts have to impose their own view on how to comply with GDPR requirements in this matter. In this regard, see Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] England and Wales High Court [EWHC] 2341 (Admin): *(146) On a complaint about a failure to comply with section 64 Data Protection Act 2018, it is for the Court to decide whether the data controller has discharged that obligation. What is required is compliance itself, i.e. not simply an attempt to comply that falls within a range of reasonable conduct. However, when determining whether the steps taken by the data controller meet the requirements of section 64, the Court will not necessarily substitute its own view for that of the data controller on all matters*.

143 Bettina Berendt and Sören Preibusch, 'Toward Accountable Discrimination-Aware Data Mining: The Importance of Keeping the Human in the Loop-and Under the Looking Glass' (2017) 5 Big Data 135, 149.

144 Federico Cabitza and others, 'The Importance of Being External. Methodological Insights for the External Validation of Machine Learning Models in Medicine' (2021) 208 Computer Methods and Programs in Biomedicine 106288.

145 Binns (n 70) 9.

146 On the use of ADM systems for crime-prevention, Selbst is optimistic too on the potential of impact assessments to design efficient human-machine collaboration systems, see Andrew D Selbst, 'Disparate Impact in Big Data Policing' (2017) 52 Georgia Law Review 109.

As we have stated above, human intervention in Article 22 GDPR is not a panacea-solution. Organisational oversight measures, such as DPIAs, must complement human oversight measures to ensure that data subjects rights are respected and guaranteed. Recently, the EDPB and the EDPS proposed that competent authorities should also be able to propose guidelines to assess bias in AI systems and assist the exercise of human oversight.[147] Those guidelines could prove helpful for controllers to adopt data protection by design strategies where the role of both human and organisational oversight shall complement each other, raising wise questions about the system's risks and impact. In our view, a post-market monitoring system –like the one designed in the Artificial Intelligence Act– could also help to identify and modify high-risk AI systems that cannot be effectively overseen by natural persons and, therefore, do not let data controllers comply with human intervention under Article 22 GDPR. While carrying out a DPIA, data controllers will collect data and evidence on whether human intervention is meaningful in the use of a high-risk AI system. And, as users under the Artificial Intelligence Act, controllers could share that gathered information with the providers to allow them to evaluate the compliance of the system with the human oversight requirement,[148] this is, to demonstrate that their high-risk AI systems can be effectively overseen by natural persons.

14. Conclusion: a myriad of pre-requisites

In this contribution we focused on the possible role of humans in ADM systems. Article 22 GDPR is a bit cryptic about human intervention, but through a bundle of methods (textual and teleological interpretations, analysis of soft law and (rare) case law), we found that:

- There are two kind of human intervention mechanisms in the GDPR. We have distinguished between Article 22(1) GDPR-decisions, that include human intervention as an essential component -in the loop- for decision-making, and Article 22(2) GDPR-decisions based solely on automated processing, that include human intervention as a safeguard -out of the loop- on request.
- Relying on the interpretation endorsed by the EDPB, for both human intervention mechanisms the kind of intervention required under the GDPR should be meaningful. More complicated has been to delve deeper into what is meaningful.
- According to WP29 Guidelines, meaningful human intervention should be carried out by someone who has the authority and competence to change the decision. Human intervention should help to ensure fairness and accuracy in decision-making considering all the relevant data; which in the case of intervention on request also must include any additional information provided by the data subject. And it should not routinely apply algorithmic outcomes, avoiding automation bias.
- To further understand the meaningfulness of human intervention, we have looked on the rationale behind Article 15 Directive 95/46/EC, the direct precedent of Article 22 GDPR. We have found that human intervention should safeguard against abdication of human responsibilities from two different perspectives. First, human intervention safeguards against data subjects' loss of control over the decisions that significantly affect them, calling for contestability. Second, human intervention safeguards against data controllers' loss of control over the decisions they take, calling for accountability.

147 EDPB-EDPS (n 57) 17. We believe that the Handbook on non-discriminating algorithms is a good model that could be followed for the guidelines mentioned by the EDPB and the EDPS. See Bart van der Sloot and others (2021). Available here: https://www.tilburguniversity.edu/about/schools/law/departments/tilt/research/handbook

148 Article 61(2) AIA: *The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.*

- This second perspective teaches us that involving humans in decision-making -in or out of the loop- aims at achieving appropriate human oversight for ADM. And that such oversight helps controllers to take responsibility for what they do with personal data, for compliance with all GDPR principles and for demonstrate this compliance.
- Data protection impact assessments (DPIA) are an indispensable tool for the enforcement of Article 22 GDPR. Many ADM systems, whether based solely on automated processing or not, will need to be subjected to a DPIA. The assessment will allow controllers to apply Article 22 GDPR correctly, choose the appropriate legal basis in the provision for ADM and the 'suitable' safeguards, including the measures to make human intervention meaningful.
- Looking at the successive initiatives of the European institutions for the regulation of AI, one can find that human oversight is a mandatory requirement for the development and use of these systems. At the same time, we note that human intervention is a necessary but not sufficient condition for an appropriate AI oversight. Human intervention will not work without human governance.
- We believe that the AIA proposal would enforce the GDPR-DPIA-system. It creates duties for AI-providers to inform users of their systems -data controllers- about essential elements such as technical measures put in place to facilitate the interpretation of the outputs of AI systems. The users are obliged by the same Act to use this information in their GDPR impact assessments.

We realise that there is still a lot of work to be done in the legal field to further develop all these ideas.

Data-driven technologies are somehow inseparably tied to the dichotomy defined by Favaretto et al., according to which humans are both the cause of its flaws and the overseers of its proper functioning.[149] The Commission does not appear to have discarded human intervention governance mechanisms as part of the solution to the problems posed by these ubiquitous technologies. Quite the contrary, regarding the analysed regulatory proposals, we have seen that these mechanisms are still very relevant to achieve human oversight. Hence, a *rarely enforced, poorly understood and easily circumvented* provision on automated decision-making is not affordable anymore for the European privacy and data protection regulatory ecosystem.

AI technologies provide *a fresh window into our democratic traditions, allowing us to better distinguish those worthy of preservation and to ask which traditions, despite their familiarity, have fallen short in practice*.[150] Involving humans in or out of the decision loops as regulatory remedies could be one of those traditions. While not forgetting the limitations that human intervention faces, in this text we argue for an interpretation that allows us to open the door to reconsider Article 22 GDPR and to claim for its relevance in the GDPR's regulatory ecosystem. In this task, we endorse a 'trial-and-error' approach[151]. If our hypothesis proved to be wrong, i.e. if it is not possible to effectively introduce meaningful and accountable human intervention for ADM systems, the GDPR regulatory ecosystem should find better remedies to achieve human oversight.

149 Favaretto, De Clercq and Elger (n 108) 21.

150 Kiel Brennan-Marquez and Stephen Henderson, 'Artificial Intelligence and Role-Reversible Judgment' (2019) 109 Journal of Criminal Law and Criminology 163.

151 *Given the limits of our knowledge and understanding, one key strategy therefore is not to rely on grand schemes, but rather to employ incremental 'trial-and-error' approaches towards regulatory change* (R. Baldwin, M. Cave & M. Lodge, 75)

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

N°24 Individuation: re-imagining data privacy laws to protect against digital harms (July 2020) by Anna Johnston (22 pages)

N°25 The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities (August 2020) by Jonas Botta (16 pages)

N°26 European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law (September 2020) by Angela Aguinaldo and Paul De Hert (16 pages)

N°27 Fashion ID and Decisively Influencing Facebook Plugins: A Fair Approach to Single and Joint Controllership (June 2021) by Paul De Hert and Georgios Bouchagiar (24 pages)

The Brussels Privacy Hub Working Papers series

N°28 Adding and removing elements of the proportionality and necessity test to achieve desired outcomes. Breyer and the necessity to end anonymity of cell phone users (September 2021) by Paul De Hert and Georgios Bouchagiar (26 pages)

N°29 Facial recognition, visual and biometric data in the US. Recent, promising developments to regulate intrusive technologies (October 2021) by Paul De Hert and Georgios Bouchagiar (46 pages)

N°30 Necessity knows no law in contaminated times: the rule of law under pandemic police and pandemic legislation' ('Nood breekt wet in besmette tijden: de rechtsstatelijkheid van de pandemiepolitie en pandemiewetgeving') (November 2021) by Paul De Hert (33 pages)

N°31 The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680 (December 2021) by Paul De Hert and Juraj Sajfert (17 pages)

N°32 Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities (January 2022) by Guillermo Lazcoz and Paul de Hert (31 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

BRUSSELS PRIVACY HUB