CHAPTER 5

Regulating Automated Decision-Making in the European Union: Article 22 GDPR and the Internal Market

Mireille M. Caruana

Abstract

In this chapter, the author will critically analyse Article 22 GDPR in light of its role as a provision intimately connected with the Internal Market and pursuing the common goal of achieving a fair and balanced digital economy that respects the rights and interests of individuals, businesses and governments. In doing so, it will engage in a critical analysis of the SCHUFA judgement (case C-634/21), the recent and first direct ruling by the CJEU on Article 22, focusing on those elements that the judgement has helped clarify and those that remain subject to considerable interpretative uncertainty, such as the right of an ex-post explanation of automated decisions.

1 Introduction[1]

The General Data Protection Regulation (GDPR) regulates certain instances of 'automated individual decision-making, including profiling'. 'Automated decision-making' refers to making a decision solely by automated means without any human involvement. In contrast, 'profiling' refers to the automated processing of personal data to evaluate an individual's personal aspects, 'such as automatic refusal of an online credit application or e-recruiting practices without human intervention.[2]

The Internal Market relies on the free movement of personal data between Member States, which is essential for economic and social integration and the development of the digital economy. Therefore, the GDPR furthers the harmonisation of rules regarding the protection of personal data in order to ensure the free flow of such data within the Internal Market. In its regulation

1 This chapter states the position as at 30th April 2024. At time of writing, the AI Act has received the approval of the European Parliament, but is still not formally enacted.

2 Recital (71) GDPR.

 | DOI:10.1163/9789004712119_007

of automated decision-making processes, the European Union aims to balance the rights of individuals and the interests of the business and government sectors, all within the ambit of the digital economy.

Article 22 of the GDPR allows automated decision-making, including profiling, only in certain circumstances, provided suitable safeguarding measures are implemented. At the same time, Article 22 of the GDPR implicitly recognises the benefits of automated decision-making for innovation, efficiency, and competitiveness in the Internal Market.

This chapter first introduces the problematics of automated decision-making and the rationale of Article 22 of the GDPR. It proceeds to an overview of the relevant articles of the GDPR regulating systems using personal data for 'automated decision-making, including profiling'. It critically analyses Article 22 of the GDPR in light of its role as a provision intimately connected with the Internal Market and pursuing the common goal of achieving a fair and balanced digital economy that respects the rights and interests of individuals, businesses and governments. Recently, the CJEU delivered its first direct ruling on Article 22,[3] clarifying some aspects, though interpretative ambiguities persist. Finally, it considers alternative provisions of the GDPR, specifically on data protection impact assessments and data protection by design, that may provide a more effective means of protection against algorithmic harms by adopting a paradigm which seeks to avert harm by ensuring the fairness and non-discriminatory nature of deployed systems.

2 Problematics of Artificial Intelligence

In February 2021, the Dutch Prime Minister and his entire cabinet resigned following a scandal concerning the use by the Dutch tax authorities of an automated decision-making algorithm to detect instances of tax fraud that resulted in thousands of families being wrongly accused of social benefits fraud 'partially due to a discriminatory algorithm' and consequently cut off from benefit payments.[4] An investigation from the Dutch Data Protection Authority found

3 Case C-634/21 *SCHUFA Holding* (*Scoring*) [2024] ECLI:EU:C:2023:957.

4 Melissa Heikkilä, *Dutch scandal serves as a warning for Europe over risks of using algorithms* (POLITICO 2022) <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/> accessed 20 March 2023; Amnesty International Report: Xenophobic Machines: Discrimination through Unregulated use of Algorithms in the Dutch Childcare Benefits Scandal (Amnesty International 2021) <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> accessed 20 March 2023.

that the algorithms deployed were discriminatory because they took variables such as whether someone had a second nationality into account.[5]

Other reports concerned the development of predictive policing technology[6] that perpetuated racial/ethnic profiling as a result of a model trained on biased and prejudiced data.[7] Amnesty International has produced a report on a pilot project called 'the Sensing Project' in the city of Roermond, dubbing the project "the automation of ethnic profiling'" and calling it "discriminatory by design".[8]

Similar reports have emerged concerning deploying AI systems in the private sector. For example, Amazon.com Inc's AMZN.O developed an algorithm that used Artificial Intelligence to review job applicants' resumès. The company realised that the system was not rating candidates for software development and other technical jobs in a gender-neutral way because the computer models were trained with data from resumès submitted to the company over ten years, most of which came from men – a reflection of male dominance across the tech industry. The model detected this pattern and replicated it.[9]

Thus, rather than overcome human bias, an AI system may merely replicate it. Worse still, in the words of the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance:

> The public perception of technology tends to be that it is inherently neutral and objective, and some have pointed out that this presumption of technological objectivity and neutrality is one that remains salient even among producers of technology. But technology is never neutral – it

5 Reported in Dutch here <https://www.volkskrant.nl/nieuws-achtergrond/belastingdienst-schuldig-aan-structurele-discriminatie-van-mensen-die-toeslagen-ontvingen~baebefdb/?referrer=https%3A%2F%2Fwww.vice.com%2F>.

6 Defined by Amnesty International as 'The application of analytical techniques across large datasets in an attempt to enable early identification of potential crime problems'. Amnesty International, *We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands* (2020) <https://www.amnesty.org/en/documents/eur35/2971/2020/en/> accessed 20 March 2023.

7 Gabriel Geiger, The Netherlands Is Becoming a Predictive Policing Hot Spot (Vice 2020) <https://www.vice.com/en/article/5dpmdd/the-netherlands-is-becoming-a-predictive-policing-hot-spot> accessed 20 March 2023.

8 Amnesty International, *We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands* (2020) <https://www.amnesty.org/en/documents/eur35/2971/2020/en/> accessed 20 March 2023.

9 Jeffrey Dastin, Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women (Reuters 2018) https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

reflects the values and interests of those who influence its design and use, and is fundamentally shaped by the same structures of inequality that operate in society.[10]

3 Rationale for Article 22 GDPR

Article 22 of the GDPR addresses the risks that may flow from automated or algorithmic decision-making. The provision closely reflects a corresponding article from the Data Protection Directive (DPD),[11] which preceded the GDPR. Animating Article 15 DPD was a "fear for the future of human dignity in the face of machine determinism".[12] This means humans should maintain ultimate control and responsibility for decisional processes that significantly affect other humans. This is brought forward in recital (4) of the GDPR, which states, "The processing of personal data should be designed to serve mankind". The foundations of the GDPR are thus embedded in fundamental human rights, essential to upholding human dignity and democratic structures.

The concern of the GDPR goes beyond issues of privacy, data protection and confidentiality to encompass other concerns relating to a broader spectrum of human rights, particularly the fundamental right of non-discrimination.[13] This is reflected in the recital (71) of the GDPR, which mentions "factors which result in inaccuracies in personal data" and the "risk of errors", as well as "the potential risks involved for the interests and rights of the data subject, (…) *inter alia*, discriminatory effects on natural persons" based on the "special categories" of personal data as defined in the GDPR and which include, for example, racial or ethnic origin, religion, genetic or health status, and sexual orientation.

10 Tendayi Achiume, *Racial discrimination and emerging digital technologies: a human rights analysis* – Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (Human Rights Council, Forty-fourth session, 15 June – 3 July 2020) A/HRC/44/57 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/151/06/PDF/G2015106.pdf?OpenElement> accessed 20 March 2023.

11 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

12 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), 249.

13 Article 21 Charter of Fundamental Rights of the European Union C 326/391.

The purpose of regulating automated decision-making is to address the risks that such algorithmic decision-making processes pose. Thinking creatively regarding safeguards, accountability, effective remedies, and redress is necessary. AI-powered 'black box' systems consisting of self-learning algorithms devoid of human oversight and supervision result in a lack of transparency, thus diminishing human control over, and responsibility for, decisional processes. Nevertheless, addressing the lack of transparency alone is not sufficient, and transparency may not be "the remedy you are looking for".[14] For example, in the context of historical data returned by the Google search engine, rather than an explanation of the decisional process, the effective remedy consisted of de-referencing by the search engine.[15]

Unfairness and discrimination through algorithms are a growing concern because of the increasing use of these systems in various sectors, coupled with the lack of regulation and transparency around their development and use. Accordingly, it is important to ensure algorithms are designed and used fairly and transparently to avoid perpetuating bias and discrimination. This may involve providing more transparency into how algorithms make decisions.

4 Article 22: Overview

In overview, Article 22 provides that:

i. the data subject has "the right not to be subject to a decision based solely on automated processing, including profiling", which produces legal or similarly significant effects;
ii. there are exceptions to this rule;
iii. where those exceptions apply, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be in place;
iv. decisions based on those exceptions must not be based on special categories of personal data listed in Article 9, unless the data subject has given explicit consent or there is a substantial public interest involved and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

14 Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.

15 Case C 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317.

5 Scope

The right in Article 22(1) applies when (1) a 'decision' is made which is (2) based solely on automated processing, including profiling and (3) produces legal effects or similarly significantly affects the data subject.

The right is operationalized by reference to 'the data subject'. In AI models, the data used to train the AI system may not include any data relating to the subject affected by the decision. Thus, the decision need not be based on data relating to that person. As the Article 29 Working Party (A29WP)[16] observes, automated decisions can be based on any data, for example:

- data provided directly by the individuals concerned (such as responses to a questionnaire);
- data observed about the individuals (such as location data collected via an application);
- derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).[17]

Nevertheless, the decision will ultimately involve data processing on that person.

5.1 *'A Decision'*

Recital 71 GDPR expounds that the data subject should have the right not to be subject to "a decision, which may include a measure (…)". A decision is the outcome of an automated processing system, while a measure is an action taken as a result of that decision. A decision can produce one or more measures, depending on the circumstances involved. A decision could be about exercising government agency authority or a private commercial entity. The term decision should be interpreted in a fairly generic sense.[18]

In the first case brought before the CJEU requiring the Court to rule directly on Article 22, a credit information service providing its customers (financial institutions) with creditworthiness assessments consisting of "the automated establishment of a probability value concerning the ability of the data subject to honour a loan in the future" without further recommendation or comment,

16 The Article 29 Working Party (A29WP), superseded by the European Data Protection Board (EDPB), issues general guidance (including guidelines, recommendations and best practice) to clarify the law and to promote common understanding of EU data protection laws. Such guidelines do not however have the force of law.

17 A29WP 2018 Guidelines, p. 8.

18 Isak Mendoza and Lee A. Bygrave 'The Right not to be Subject to Automated Decisions based on Profiling', in Synodinou, Jougleux, Markou and Prastitou (eds.), *EU Internet Law: Regulation and Enforcement* (Springer 2017) 87.

claimed that it only provides information to its customers, who in turn take the actual decisions concerning credit agreements. As defined by the AG, the matter concerned "whether the decision-making procedure is designed in such a way that the scoring carried out by the commercial information company predetermines the decision of the financial institution to grant or refuse credit".[19] If in its decision-making procedure the financial institution gives paramount importance to the scoring transmitted by the credit information service, and since a negative score can, on its own, produce unfavourable effects for the person concerned, qualifying it as a 'decision' seems justified. In this instance, the facts of the case indicate that the scores established by the credit information service and communicated to the financial institution play a decisive or determining role when granting loans and designing their conditions.[20] It follows that the score itself must be considered as having the quality of a 'decision' within the meaning of Article 22(1) GDPR.[21] The AG opined that this is essentially a question of fact which can best be assessed by the national courts in each particular case, as the answer to this question depends on internal rules and practices of the financial institution in question, which must generally leave it no leeway as to the application of the score to a credit application.[22]

5.2 *'Based Solely on Automated Processing, Including Profiling'*

Article 22(1) applies only to decisions based 'solely' on automated processing. While the initial data capture may not be fully automated but could be manual or semi-automated, Article 22 would still be engaged, provided the data upon which the decision is based are digital.

A decision is not considered to be based 'solely' on automated processing if there is human involvement. The A29WP considers that to qualify as human involvement, "the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. Someone should do it with the authority and competence to change the decision".[23] Thus, a decisional support tool falls clear of Article 22.

---

19 C-634/21 *Shufa Holding* (*Scoring*) [2023] ECLI:EU:C:2023:220, Opinion of AG Pikamae, para 42. Note: The Advocate General's Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are responsible.

20 C-634/21 *Shufa*, Opinion (n 19) para 43, paras 46–52.

21 C-634/21 *Shufa*, Opinion (n 19) para 47.

22 C-634/21 *Shufa*, Opinion (n 19) para 44.

23 A29WP 2018 Guidelines, 21.

This matter was at issue in the *SCHUFA Holding* (*Scoring*) case. While from the facts of the case, it appeared that the creditworthiness assessment conducted by SCHUFA is indeed fully automated, the financial institution to which SCHUFA communicates the score is called upon to adopt an ostensibly autonomous act with regard to the person concerned, namely the granting or refusal of credit. Therefore, should SCHUFA's profiling procedure (and subsequent assessment) be viewed as a decisional support tool for credit granting (or refusal), Article 22 would not be engaged. Referring to the facts of the case[24] and making an argument for effective protection,[25] the Advocate General concluded that a "decision based solely on automated processing' is indeed taken by SCHUFA, as 'in accordance with consistent practice" the financial institution "bases its decision relating to the establishment, the execution or termination of a contractual relationship with this same person in a decisive manner on said value".[26]

In a case concerning Uber drivers who challenged the deactivation of their accounts and consequent termination of their contracts due to alleged fraudulent actions, the Amsterdam District Court concluded that there were no fully automated decisions. The applicants did not contest Uber's explanations about their decision-making process, and thus, they were accepted by the court. Uber stated that the relevant decisions were made by (at least) two employees of the risk team based on an investigation conducted by an employee in response to fraud signals. One of those decisions was even made after an Uber employee investigated the signals about using the manipulated app and spoke to the driver. The Court ruled that this involved significant human intervention.[27] The Court consequently denied the drivers access to meaningful information concerning the algorithm according to Article 15 of the GDPR.[28]

The scope of the provision embraces decisions based solely on automated processing that may, but need not, involve profiling. Article 4(4) GDPR defines 'profiling' as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural

24 C-634/21 *Shufa*, Opinion (n 19) para 46.

25 C-634/21 *Shufa*, Opinion (n 19) paras 48–51.

26 C-634/21 *Shufa*, Opinion (n 19) para 59.

27 Uber deactivation judgement, para 4.24. Unofficial English translations available: <https://ekker.legal/en/2021/03/13/dutch-Court-rules-on-data-transparency-for-uber-and-ola-drivers/> accessed 21 March 2023.

28 Uber deactivation judgement, para 4.26. For commentary see: Raphaël Gellert, Marvin van Bekkum, and Frederik Zuiderveen Borgesius, 'The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making' (EU Law Analysis, 28 April 2021) <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html> accessed 21 March 2023.

person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". In the SCHUFA (Scoring) case, Advocate General Pikamäe opined that the automated establishment of a credit score, which reflects a probability concerning an individual's likelihood to repay a loan in the future, constitutes profiling under the GDPR.[29] The CJEU confirmed this.[30] In practice, many, if not most, types of automated decision-making will include profiling.[31]

5.3 *Producing 'Legal Effects' or 'Similarly Significant Effects' for the Interested Party*

Applying Article 22(1) requires that the decision has serious consequences for the data subject insofar as it produces "legal" or "similarly significant" effects. A legal effect requires that the decision affects the data subject's legal rights, legal status or rights under a contract. Examples of 'legal effects' include automated decisions about an individual that result in:

– the establishment, execution or termination of a contractual relationship;
– entitlement to or denial of a particular social benefit granted by law, such as a child or housing benefit;
– refused admission to a country or denial of citizenship.[32]

Using the word 'similarly' in 'similarly significant effects' ties the notion of 'significant effects' to 'legal effects'. Therefore, only the effects that have a serious impact will be covered by this provision.[33] In the Opinion of the Article 29 Working Party (A29WP), subsequently endorsed by the European Data Protection Board (EDPB), a 'significant' effect is produced when a decision has the potential to

– significantly affect the circumstances, behaviour or choices of the individuals concerned;
– have a prolonged or permanent impact on the data subject or
– at its most extreme, lead to the exclusion or discrimination of individuals.[34]

---

29 C-634/21 *Shufa*, Opinion (n 19) para 33.

30 Case C-634/21 *SCHUFA Holding* (*Scoring*) [2024] ECLI:EU:C:2023:957, para 47.

31 Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27(2) International Journal of Law and Information Technology 91, 97.

32 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018. WP251rev.01, 21.

33 C-634/21 *Shufa*, Opinion (n 19) para 34.

34 EDPB, Endorsement 1/2018 (25 May 2018) (endorsing Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018. WP251rev.01), 21.

The EDPB opines that the following decisions could fall into this category:
- decisions that affect someone's financial circumstances, such as their eligibility for credit;
- decisions that affect someone's access to health services;
- decisions that deny someone an employment opportunity or put them at a serious disadvantage;
- decisions that affect someone's access to education, such as university admissions.[35]

The SCHUFA case concerned precisely a decision that affected someone's financial circumstances. Indeed, AG Pikamäe noted that the decision made by the credit information service provider produces both 'legal' and 'economic' effects. Insofar as it constitutes a step prior to the conclusion of a loan contract, the economic consequences are such that they produce effects that are similarly significant as the legal effects.[36]

Another concrete instance of a situation where a court found a "legal or similarly significant effect" to be produced by an automated decision-making system was the system employed by Ola, a ridesharing company, that resulted in the imposition of penalties and deductions.[37] The Amsterdam District Court ruled that the decision to impose a discount or fine has "effects that are important enough to merit attention and that significantly affect the behaviour or choices of the person concerned as referred to in the Guidelines".[38] The automated decision led to a sanction that affected the data subject's rights under the agreement with Ola. However, with regard to the driver's 'earning profile' aspect of the same automated system that resulted in decisions to award (or withhold) a bonus, the same Court ruled that "Although the possibility of obtaining a bonus will have some influence on the driver's behaviour, it has not been shown to have legal or significant effects as referred to in the Guidelines".[39] The latter conclusion was also reached with regard to the 'Guardian'

35 EDPB, Endorsement 1/2018 (25 May 2018) (endorsing Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018. WP251rev.01), 22.

36 C-634/21 *Shufa*, Opinion (n 19) para 35.

37 Amsterdam District Court, 11 March 2021, C / 13/689705 / HA RK 20-258, para 4.51.

38 *Ibid*. [unofficial English translations available <https://ekker.legal/en/2021/03/13/dutch-Court-rules-on-data-transparency-for-uber-and-ola-drivers/>].

39 Amsterdam District Court, 11 March 2021, C / 13/689705 / HA RK 20-258, para 4.47 [unofficial English translations available <https://ekker.legal/en/2021/03/13/dutch-Court-rules-on-data-transparency-for-uber-and-ola-drivers/>].

system to detect irregularities, used to monitor journeys to promote driver and passenger safety,[40] and the system for assigning trips.[41]

In the *Uber* (employment) judgement, the same Amsterdam District Court examined the algorithm-mediated matching of drivers and passengers to allocate available rides. In the Court's view, the drivers did not adequately motivate why there was a 'legal' or 'significant effect' as per Article 22 GDPR.[42]

The linkage of legal and 'similarly' significant effects leads to doubts concerning whether behaviourally targeted advertising will ordinarily meet the significant effects threshold. The decision to present targeted advertising based on profiling will not usually have a 'legal or similarly significant effect' on individuals. However, depending on the particular characteristics, it may potentially have such 'similarly significant' effects. The A29WP/EDPB highlight the following characteristics:

– the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
– the expectations and wishes of the individuals concerned;
– the way the advert is delivered or
– using knowledge of the vulnerabilities of the data subjects targeted.[43]

Such targeted advertising might, therefore, meet the 'similarly significant' threshold if 'it involved blatantly unfair discrimination with non-trivial economic consequences'.[44]

Moreover, the 'significant effects' contemplated in the legal provision are measured in relation to the individual data subject concerned rather than by reference to the 'average' person. In the context of a discussion on whether targeted advertising may, in principle or a particular instance, have a 'similarly significant effect' on a data subject, Brkan opines that Article 22 GDPR requires that "the decision significantly affects a particular data subject ('him or her') and not an average one".[45] Considering the 'average' rather than the actual consumer targeted with the advertising "might not take into account particular

40 Amsterdam District Court, 11 March 2021, C / 13/689705 / HA RK 20-258, para 4.48–4.49.
41 Amsterdam District Court, 11 March 2021, C / 13/689705 / HA RK 20-258, para 4.50.
42 Amsterdam District Court, 11 March 2021, C / 13/687315 / HA RK 20-207, para 4.66–4.67.
43 A29WP 2018 22.
44 Lee A. Bygrave 'Article 22. Automated individual decision-making including profiling' in *The EU General Data Protection Regulation* (*GDPR*) *A Commentary* (OUP 2020) 534–5.
45 Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27(2) International Journal of Law and Information Technology 91, 103.

vulnerabilities of a data subject, such as sicknesses, addictions, anxieties or traumatic past experiences".[46]

Individual harm can also result from group harm because of the attributes of a particular group to which the individual belongs and which is relevant to the decision made. An automated decision may have 'significant effects' on individuals as members of a group, for example, if a person's creditworthiness is determined not by her or his individual credit history but rather by his geophysical address.

When the affected/harmed group consists of a vulnerable group, such as children, this lowers the threshold of 'similarly significant effects'. Recital (38) GDPR posits that "children merit specific protection with regard to their personal data" and that such protection should "in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles". Furthermore, recital (71) expands that a measure evaluating personal aspects based solely on automated processing and which produces legal or similarly significant effects "should not concern a child".

6 Right or Prohibition?

An ongoing controversy in the literature concerns whether the enigmatic 'right not to be subject' to an automated decision is to be interpreted as a general, qualified prohibition or rather as a *right* to be exercised at the data subject's discretion. The A29WP has interpreted Article 22(1) as establishing a *general prohibition* on fully automated individual decision-making, including profiling with a legal or similarly significant effect.[47]

However, academic opinion on this matter is divided. It has been convincingly argued that "such a provision is better characterized as conferring upon data subjects a right that they may exercise at their discretion, rather than establishing a general ban on individual decisions based solely on automated processing".[48] This interpretation is strongly supported by the fact that other provisions of the GDPR assume the existence of this type of processing; for example, the transparency duties, which require the communication

46 *Ibid.*

47 A29WP 2018, p.19. "Interpreting Article 22 as a prohibition rather than a right to be invoked means that individuals are automatically protected from the potential effects this type of processing may have". A29WP 2018, 20.

48 Luca Tosoni. The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*, 2021, Vol. 11, No. 2.

of information to the data subject regarding "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4)". Furthermore, this interpretation is consistent with the widespread deployment of such systems in both the public and private sectors where digitalization is advanced and where there may be socially justifiable benefits.[49]

Despite the convincing nature of the latter view (indeed, Bygrave opines that *lex lata* "the better view" is that Article 22(1) provides a right to be exercised at the discretion of data subjects[50]), the AG advised the Court to take a different direction and opt for a reading of Article 22(1) as a "general prohibition" of automated decision-making producing legal effects concerning or significantly affecting the data subject similarly. While acknowledging that Article 22(1) GDPR is 'special' compared to the other restrictions on the processing of data contained in the GDPR, in that it enshrines a 'right' of the data subject not to be subject to a decision based solely on automated processing, the AG opined that, notwithstanding the terminology used, the application of Article 22(1) GDPR does not require the data subject to actively invoke the right. Rather, considering the scheme of that provision, in particular paragraph 2, which sets out the cases in which such automated processing is exceptionally authorized, the provision allows the conclusion that the said provision establishes a general prohibition of decisions of the type described above.[51] The CJEU has concurred that Article 22 'lays down a prohibition in principle, the infringement of which does not need to be invoked individually by such a person'.[52]

7 Exceptions to Article 22(1)

Article 22(2) provides exceptions from Article 22(1). The latter does 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.

49 Bygrave, 'Minding the Machine v2.0' (n 12) 253.

50 Lee A. Bygrave, 'Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions' in Ienca et al. (eds.), Cambridge Handbook of Information Technology, Life Sciences and Human Rights. Cambridge University Press 2022.

51 C-634/21 *Shufa*, Opinion (n 19) para 31.

52 SCHUFA Holding (n 3) para 52.

Where the individual has consented to such decisions, or if such decisions are necessary for entering into, or performing, a contract between the individual and the company, the data controller must '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'.[53]

7.1 *Contracts*

The contractual derogation under Article 22(2) includes a 'necessity' criterion that "signals at least that the decision must have been *required* for entering into or fulfilling the contract with the data subject".[54] Mendoza and Bygrave comment, "The rationale behind the criterion is presumably to make it difficult for the data controller to escape Article 22(1) by merely pointing to a standardised contract with the data subject".[55]

A key operational issue remains regarding the precise meaning of the 'necessity' criterion in the provisions of the GDPR. Notably, 'necessary' is not as stringent and restricting as 'indispensable'. In *Huber*,[56] the CJEU assessed whether a centralized database was necessary in terms of *effectiveness*:

> … the centralisation of those data **could be necessary**, within the meaning of Article 7(e) of Directive 95/46, if it contributes to the more **effective** application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals.

Although this judgment interprets Article 7(e) Directive 95/46, the terminology of 'necessity' is used in both the GDPR and the Directive that preceded it; accordingly, the same interpretation should be applied if a new case requires a similar or equivalent assessment.

7.2 *Statutory Authority*

National legislation will likely play a major part in determining the level of protection under Article 22. Any such national legislation must provide "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". The A29WP assumes that the safeguards that will be provided for

53 Article 22(3) GDPR.
54 Bygrave, *A Commentary* (n 44) 536.
55 Mendoza and Bygrave (n 18) 92.
56 C-524/06 Huber ECLI:EU:C:2008:724.

under statutory authority will be of the same nature as those provided for where the exceptions of contract or consent apply, and thus: "such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision", noting that "human intervention is a key element".[57] Authorization by Member State law is nevertheless likely to result in significant divergence between national legislative regimes, which is not ideal given the Digital Single Market ideal pursued by the GDPR.

7.3 *Consent*

The third derogation listed in Article 22(2) concerns a decision based on the data subject's 'explicit' consent. Article 4(11) GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Furthermore, Article 7 GDPR on the conditions for consent, provides that "When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract or provision of that service".[58] It is, therefore, relevant to consider whether conditional automated decision-making is necessary for the performance of that contract. The data subject's interest in that contract is also relevant. For example, suppose the data subject applies for credit or insurance. In that case, the fact that the contract is in the data subject's interest makes it easier to argue that consent is freely given than when the decision is not.

7.4 *Safeguards*

In cases where the exceptions of contract and consent apply, the data controller must implement suitable safeguards, which must consist of 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.[59] Therefore, the data subject should always have the right to demand a human review of an automated decision. Mendoza and Bygrave posit that "these rights (particularly that of human involvement) mean that there will be insignificant difference in the level of

57 A29WP 2018 *Guidelines*, 27.
58 Article 7(4) GDPR; cf. recital (43).
59 Article 22(3) GDPR.

protection between the right/prohibition in Article 22(1) and the exceptions".[60] In a similar vein, Bygrave concludes that: "there will ultimately be very little difference between the level of protection offered by the exercise of the 'right' in Article 22(1) and that offered by the exercise of the rights in Article 22(3), particularly in the situation where the former 'right' is exercised *ex-post* (i.e. after a decision is adopted)".[61]

The list of essential safeguards found in Article 22(3) is not exhaustive; other safeguards may be implemented that are not listed there. In particular, whether a 'right to an explanation' of a particular decision is a safeguard that the GDPR mandates has been the subject of much debate and controversy.

8 A 'Right to an Explanation'?

The controversy surrounding the existence or otherwise of a 'right to an explanation' emerges from a reading of Article 22(3) in light of the recital (71), which provides that "such processing should be subject to suitable safeguards, which should include [the right] to obtain an explanation of the decision reached after such assessment". It should be recalled, however, that recitals have no binding legal force.[62] They are merely "interpretative tools in the EU legal order" that "help to explain the purpose and intent behind a normative instrument" and "can also be taken into account to resolve ambiguities in the legislative provisions to which they relate". Nevertheless, a recital "cannot displace the operative provisions of a legal instrument".[63]

This has resulted in considerable controversy over the question of the nature and existence of such a 'right to an explanation' under the GDPR.[64] If such a right exists, it is nevertheless unclear whether this right consists of an

60 Mendoza and Bygrave (n 18) 92.

61 Bygrave, *A Commentary* (n 44) 538.

62 Case C-162/97, Nilsson, [1998] ECLI:EU:C:1998:554, para 54.

63 Roberto Baratta, 'Complexity of EU law in the domestic implementing process' [2014] 19th Quality of Legislation Seminar – EU Legislative Drafting: Views from those applying EU law in the Member States <https://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf> references excluded, accessed 9 February 2023.

64 Brybe Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38(3) AI Magazine 50 ('any adequate explanation would, at a minimum, provide an account of how input features relate to predictions …' at p. 29); 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; Andrew D Selbst and Julia Powles, 'Meaningful information and the right to explanation' (2017) 7(4) International Data Privacy Law 233.

explanation of specific decisions (*ex-post* explanation) or an explanation of system functionality. Moreover, uncertainty surrounds the question of the extent to which companies must disclose information about their algorithms and how this obligation is to be balanced with the company's right to intellectual property protection,[65] including trade secrets. Furthermore, the extent to which an ML operation and/or output can be explained at all is doubtful,[66] and it is, in any case, doubtful whether an overly complex explanation would comply with the principle of transparency.

Insofar as transparency is concerned, Article 13 of the GDPR provides that a controller is obliged to provide the data subject with specified information when personal data are obtained, where information is collected from a data subject. In particular, the controller must inform the data subject of "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, *meaningful information about the logic involved*, as well as the significance and the envisaged consequences of such processing for the data subject".[67] An identical information requirement is found in Article 14 of the GDPR, which provides information requirements where personal data have not been obtained from the data subject (but from a third party).[68] Both Articles 13 and 14 envisage the provision of this information at the time of processing and would thus seem to indicate that what is being envisaged is not a right to an explanation of a particular decision, and, because of the requirement to provide "meaningful information about the logic involved", "not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm".[69]

Beyond Articles 13 and 14, Article 15 GDPR provides for the right of a data subject to have access to the personal data concerning him or her that are processed by a controller, including information concerning "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".[70] While the data subject's right of access under Article 15 would be exercised after the processing has commenced,

65 See Art 17 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

66 See EDPS, TechDispatch #2/2023 – Explainable Artificial Intelligence (16 November 2023) <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en#:~:text=Explainable%20Artificial%20Intelligence%20(XAI)%20is,of%20their%20decision%2Dmaking%20processes> accessed 24 April 2024.

67 Art 13(2)(f) GDPR [author's emphasis].

68 Art 14(2)(g) GDPR.

69 A29WP 2018, 25.

70 Art 15(1)(h) GDPR.

the identical wording to that found in Articles 13 and 14 has led the A29WP to conclude that the interpretation of the equivalent element under Article 15 should be interpreted in the same way, and thus that there is no *ex post* right to an explanation of a particular decision. The fact that the provision speaks of "the significance and envisaged consequences" of the processing indicates that this is not an *ex-post* explanation of a particular decision.[71] Nevertheless, in the opinion of the A29WP, the controller should "provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision".[72]

In line with the view of the A29WP, Mendoza and Bygrave posit that "we should not discount the possibility that a right of *ex-post* explanation of automated decisions is implicit in the right 'to contest' a decision pursuant to Article 22(3)".[73] If a data subject wants to contest a decision, at a minimum, they need to be heard and the merits of the contestation considered by the decision-maker. Such a process would not be fair if the decision-maker were not subject to a qualified obligation[74] to give reasons for (or an explanation of) the decision.[75] Furthermore, the obligation to give reasons is buttressed by the core data protection principle of "fairness, lawfulness and transparency", which is given effect in various GDPR provisions, including Article 22.

The AG Opinion in the *SCHUFA* case[76] reflects this author's conclusions based on the above considerations. In that case, *SCHUFA*, the credit information service provider, refused to disclose the various elements taken into account to calculate the creditworthiness assessment score and their weighting, referring to trade secrecy. The AG posited that Article 15(1)(h) must be interpreted as meaning that it covers, in principle, also the method of calculation used by a commercial information company to establish the credit score, provided that there are no conflicting interests worthy of protection. In this respect, the AG pointed towards recital (63) GDPR, which states that the right of access "should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software".[77] The AG opined that a 'fair balance' between competing interests must be sought. Moreover, recital (63) states that "the result of those

71 A29WP 2018, 27.
72 *Ibid.*
73 Mendoza and Bygrave (n 18) 93–94.
74 See Article 23 GDPR on restrictions to data subject rights.
75 Mendoza and Bygrave (n 18) 93–94.
76 C-634/21 *Shufa*, Opinion (n 19).
77 C-634/21 *Shufa*, Opinion (n 19) para 54.

considerations should not be a refusal to provide all information to the data subject". Reading Article 15(1)(h) in light of the transparency requirements of Article 12, and in particular that the data subject should receive information that is understandable and accessible, the AG excluded a possible obligation to disclose the algorithm, given its complexity, emphasizing that "the usefulness of communicating a particularly complex formula would be doubtful without providing the necessary explanations".[78] Thus the Article 15(1)(h) obligation:

> must be understood as meaning that it includes *sufficiently detailed explanations of the method used for the calculation of the score and the reasons that led to a particular result*. In general, the data controller should provide the data subject with aggregate information, in particular on the factors taken into consideration for the decision-making process and their respective importance at an aggregate level, which is also useful for him to challenge any "decision" in the sense of Article 22(1) GDPR.[79]

This line of interpretation was also previously upheld by the Amsterdam District Court, which required Ola to explain the logic behind a fully automated decision. That Court also referred to the A29WP Guidelines, interpreting Article 15(1)(h) to mean that "the main assessment criteria and their role in the automated decision" must be communicated to the data subjects "so that they can understand the criteria based on which the decisions were taken, and they can check the correctness and lawfulness of the data processing".[80]

Summarising, the position at law is as follows:

i. Requirement to disclose 'meaningful information' or an 'explanation' of system functionality that is sufficiently detailed as to enable a right to contest the decision as per Article 22(3);
ii. Coupled with a right of access to personal data processed relating to the data subject, an explanation of system functionality should lead to an explanation of the specific decision made;
iii. There is no requirement to disclose the algorithm;
iv. It requires a balancing of interests of the data subject and the controller (in particular, data protection and intellectual property-related interests).

78 *Ibid*., para 57.
79 *Ibid*., para 58 (emphasis added).
80 Amsterdam District Court, 11 March 2021, C / 13/689705 / HA RK 20-258, para 4.47 [unofficial English translations available <https://ekker.legal/en/2021/03/13/dutch-Court-rules-on-data-transparency-for-uber-and-ola-drivers/>] para 4.52.

9 Limitations of the 'Right to an Explanation'

The data subject's right to receive an explanation may be restricted per Article 23 of the GDPR.[81] As aforementioned, this may prevent undue prejudice to the rights and legitimate interests of the decision-maker, particularly regarding intellectual property rights, such as trade secrets. Nevertheless, the principle of transparency expounded in the recital (58) is highly relevant in "situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether by whom and for what purpose personal data relating to him or her are being collected".

Thus, seeking a fair balance between competing rights and responsibilities is necessary, considering the fundamental nature of both data protection rights and intellectual property.[82] The Advocate General in the *SCHUFA* case considered that the obligation to provide "meaningful information about the logic involved" should be read in light of the aforementioned recitals and that:

> A minimum of information must in any case be provided in order not to compromise the essential content of the right to the protection of personal data. (…) [I]f the protection of trade secrecy or intellectual property constitutes, in principle, for a commercial information company a legitimate reason to refuse to reveal the algorithm used to calculate the score of the data subject, (…) it can in no way justify an absolute refusal of information. More so, when there are appropriate means of communication, which facilitate understanding while guaranteeing a certain degree of confidentiality'.[83]

10 Prohibitions of Decisions Based on "Special Categories of Personal Data"

Article 22(4) prohibits automated decision-making based on "special categories of personal data".[84] While this supersedes the exceptions listed in Article 22(2), it is a qualified prohibition as there are another two exceptions: if

81 Art 23(1)(i) GDPR.

82 Art 8 on the protection of personal data and Art 17 on the Right to property (including intellectual property) Charter of Fundamental Rights of the European Union.

83 C-634/21 *Shufa*, Opinion (n 19) para 56 (my translation).

84 Defined in Article 9(1) GDPR.

the data subject has given explicit consent to the processing of those personal data under Article 9(1)(a); and if the processing is necessary for reasons of substantial public interest under Article 9(1)(g). In the latter case, the processing must be provided for by Union or Member State law and be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Furthermore, "suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests" must be in both cases. These requirements are identical in wording to those found in Article 22(2) and (3) and should thus presumably be interpreted similarly.

11 Rights for Groups and Society

Data protection legislation has emerged from a human rights paradigm, thus focusing mainly on individual rights. It is important, however, to acknowledge the limitations of the individual rights paradigm to consider rights for groups and society more broadly, as well as the tools in data protection law's arsenal that uphold such broader rights. Moreover, data protection law moves beyond its foundational concern with privacy-related interests to encompass concerns about averting discriminatory effects. This is evidenced in the text of a recital of the GDPR:

> the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, *inter alia*, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect.[85]

One might ponder the efficacy of exercising individual rights, like the 'right to an explanation', and question whether these rights truly offer a meaningful remedy across various situations. Furthermore, transparency is largely

85 Recital (71) GDPR.

inadequate for understanding and governing algorithmic systems, given the complexities of societal power dynamics and institutions, leading to potential societal or algorithmic harms. Hence, there is a need to guard against the 'transparency fallacy', wherein the anticipated advantages of apparent transparency prove illusory due to individuals being predominantly time – and resource-constrained and often lacking the requisite expertise to exercise these rights effectively.[86] Thus, it becomes essential to go beyond individual rights and shift our focus towards algorithmic governance.[87]

12 Impact Assessments

An impact assessment is an *ex-ante* systematic evaluation process used to analyse the potential consequences of a proposed action, policy, project, or decision on various social, environmental, economic, and legal factors. The GDPR establishes the mandatory requirement of carrying out a 'data protection impact assessment' (DPIA) in case of processing likely to result in a high-risk to data subjects: "Where a type of 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".[88] It is further specified that a DPIA is required in particular in the case of a 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'[89] and "processing on a large scale of special categories of data".[90] A DPIA proves invaluable in crafting the requisite safeguards in alignment with the stipulations outlined in Article 22 of the GDPR. Furthermore, where the DPIA indicates that the processing "would result in a high risk in the absence of measures taken by the controller to mitigate the risk", the

86 Edwards and Veale (n 14).

87 Mike Ananny and Kate Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' (2018) 20(3) New Media & Society 973.

88 Article 35(1) GDPR; See A29WP *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* (wp248rev.01) Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017 <https://ec.europa.eu/newsroom/article29/items/611236/en>.

89 Art 35(3)(a) GDPR.

90 Art 35(3)(c) GDPR.

controller must consult the supervisory authority before the start of processing activities.[91] The supervisory authority would, in turn, be able to exercise its powers, including imposing a temporary or definitive limitation, such as a ban on processing.[92] Thus, a decisional system may be banned *ex-ante* (and fines imposed upon non-compliant controllers[93]).

A weakness of this requirement is that it is premised on the controller's self-assessment of the nature of the risk of the processing. Nevertheless, 'high-risk' technologies are almost certain to capture most predictive analytics or ML systems. However, one should also note that a DPIA is not a comprehensive *ex-ante* fundamental rights-based impact assessment; that is, a human rights impact assessment emphasising elements such as fairness, equality and non-discrimination. 'Algorithmic Impact Assessments' have been proposed to link individual rights and systemic governance,[94] thus providing algorithmic accountability. While not yet a requirement for all AI systems, this obligation is anticipated to be instituted for systems classified as 'high-risk' with the enactment of the AI Act.[95]

13 'By Design' Strategies

'By design' strategies refer to the deliberate incorporation of legal principles, safeguards, and mechanisms into the fundamental structure and development process of systems, products, or services to ensure compliance and mitigate risks from the outset. For example, 'data protection by design' entails integrating privacy and security measures into the development process of systems, products, or services from their inception. Article 25 of the GDPR provides an obligation for the controller to "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, effectively and to integrate the necessary safeguards into the processing in order to meet the

91 Art 36(1) GDPR.

92 Art 58(2)(f) GDPR.

93 Art 83 GDPR.

94 Margot E Kaminski, Gianclaudio Malgieri, Algorithmic impact assessments under the GDPR: producing multi-layered explanations, *International Data Privacy Law*, Volume 11, Issue 2, April 2021, 125–144.

95 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. The AI Act was formally adopted by Parliament on 13 March 2024.

requirements of this Regulation and protect the rights of data subjects". This obligation exists "both at the time of determining the means for processing and at the time of the processing itself".[96] The obligation imposed by Article 25 is qualified by an extensive list of contextual factors: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". These will be determined largely by the data protection impact assessment that controllers engaging in processing that is "likely to result in a high risk" to persons' rights and freedoms are required to conduct according to Article 35 above. Thus, there is a link between impact assessments and Article 25 requirements.

14 Accountability: *Ex-ante* Impact Assessments, *Post-Factum* Audits and Effective Remedies

Through initiatives like impact assessments, 'by design' strategies, and others such as codes of conduct[97] and certification,[98] increased accountability for unfairness, discrimination, and reparations to affected individuals and communities are anticipated. However, some organizational difficulties need to be overcome. For instance, determining responsibility for reviewing audit trails raises questions about whether it should be assigned to an external regulator like the supervisory authorities established under the GDPR or an audit body. Moreover, implementing and enforcing such requirements in the private sector poses greater challenges. Further considerations include the risk of excessive bureaucratic burdens that do not translate into effective heightened substantive protection for data subjects.

15 Conclusion

This book chapter has explored the societal risks associated with automated individual decision-making, including profiling, and the rationale for its regulation through data protection legislation, particularly emphasising Article 22 of the GDPR and its role within the Internal Market. Through a critical analysis of this provision, drawing on interpretative case law such as the

96 Article 25 GDPR.
97 See Art 40 GDPR.
98 See Art 42 GDPR.

recent CJEU *SCHUFA* ruling, the chapter situates the regulation of automated decision-making within a broader context. It has considered other GDPR provisions to foster safe technological systems to prevent harm rather than solely providing retrospective remedies. These considerations have been central since the enactment of the GDPR in 2016, with evolving discourse. This discourse has culminated in the proposal for an AI Act, which, after a protracted legislative process, nears enactment. Notably, the AI Act introduces mandatory 'fundamental rights impact assessments'[99] and a 'right to an explanation of individual decision-making'[100] for 'high-risk' AI systems.[101] A discussion on the implications of the AI Act on the regulation of AI systems is beyond the scope of this chapter but is addressed in the following one.

Bibliography

Ananny M and K Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability' (2018) 20(3) *New Media & Society* 973.

Barros Vale S and G Zanfir-Fortuna, 'Automated Decision-Making under the GDPR: Practical Cases from Courts and Data Protection Authorities' (The Future of Privacy Forum 2022) <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf>

Bincoletto G, 'Italy – Supreme Court of Cassation on Automated Decision Making: Invalid Consent If an Algorithm Is Not Transparent' (2021) 7 *European Data Protection Law Review* 248 < https://edpl.lexxion.eu/data/article/17345/pdf/edpl_2021_02-017.pdf>

Brkan M, 'Do Algorithms Rule the World? Algorithmic Decision Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27(2) *International Journal of Law and Information Technology* 91.

Bygrave L A, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17(1) *Computer Law & Security Review*, 17.

Edwards L and M Veale, Slave to the Algorithm? Why a 'Right To an Explanation' Is Probably Not the Remedy You Are Looking For (2017) 16(1) *Duke Law & Technology Review* 18.

Gellert, R, M van Bekkum, and F Z Borgesius, 'The Ola & Uber judgements: for the first time a court recognises a GDPR right to an explanation for algorithmic

99 Art 27 AI Act.

100 Art 86 AI Act.

101 Defined in Art 6 AI Act.

decision-making' EU Law Analysis (2021) <http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html>

Goodman B and S Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2016) ICML Workshop on Human Interpretability in Machine Learning, arXiv:1606.08813 (v3); (2017) 38 *AI Magazine* 50.

Hawath M, '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.

Kaminski M E and G Malgieri, 'Algorithmic impact assessments under the GDPR: producing multi-layered explanations' (2021) 11(2) *International Data Privacy Law* 125.

Malgieri G, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35(5) *Computer Law & Security Review* 105327 <https://www.sciencedirect.com/science/article/pii/S0267364918303753>

Mendoza I and L A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling', in Synodinou, Jougleux, Markou and Prastitou (eds.), *EU Internet Law: Regulation and Enforcement* (Springer 2017), 77.

Sartor G, 'The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Selbst, A D and J Powles, 'Meaningful information and the right to explanation' (2017) 7(4) *International Data Privacy Law* 233.

Van Bekkum, M and F Z Borgesius, 'Digital Welfare Fraud Detection and the Dutch SyRI Judgment' (2021) 23 *European Journal of Social Security* 323 <https://journals.sagepub.com/doi/10.1177/13882627211031257#bibr13-13882627211031257>

Wachter S, B Mittelstadt and L Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (2017) 7(2) *International Data Privacy Law* 76.

Official Publications

A29WP 2018: Article 29 Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251, 3 October 2017) As last Revised and Adopted on 6 February 2018. WP251rev.01.

A29WP 2017: Article 29 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* (wp248rev.01) Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017 <https://ec.europa.eu/newsroom/article29/items/611236/en>

List of Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.