eLaw
Working Paper Series

No 202ť/00" - ELAW– 202ť

a zpq~ ¡mzpuzs,¡tq,xqsmx,nm q ,r{~,m¢¡{ y m¡qp, pqou u{z9y mwuzs,¢zpq~,¡tq,S P \ ^

ZuÀq£u˘8, Y :8,_qm~ 8,M: Y :8,R{ ot9buxxm~{zsm8,Q:8,O¢ ¡q~ 8, N:T:Y:,

Universiteit Leiden
eLaw

Discover the world at Leiden University

Pre-print version - cite as:
•Nišević, M., Sears, A.M., Fosch-Villaronga, E., Custers, B.H.M. (2022) Understanding the legal bases for automated decision-making under the GDPR, in: E. Kosta, R. Leenes, I. Kamara (eds.) Research handbook on EU data protection, Cheltenham: Edward Elgar Publishing, p. 435-454.

17. Understanding the legal bases for automated decision-making under the GDPR

Maja Nišević, Alan M. Sears, Eduard Fosch-Villaronga and Bart Custers

1. INTRODUCTION

Governments and organizations around the globe employ profiling and inferential analytics methods to surmise the characteristics and preferences of individuals.[1] By knowing users' characteristics, organizations can make their practices more precise and effective, targeting or excluding certain groups more efficiently, personalizing online behavioural advertising, and increasing users' time on their platforms.[2] Similarly, governments can use such detailed information to improve their services, predict crime, or anticipate risky behavior.[3] These techniques are useful to analyse vast volumes of data and provide detailed information on citizens worldwide, including sensitive attributes such as race, gender, sexual orientation, and political opinion, predicting individuals' preferences and future behaviour.[4] They have also been effective in supporting ulterior decision-making processes such as automatic online credit applications, e-recruiting practices, or diagnoses of certain diseases.

While the analysis of such amounts of data through automated means can lead to quick, standard, and consistent decisions—also called automated-decision making, or ADM—these decisions can significantly affect individuals in various ways.[5] Moreover, inferential analytics are often opaque and assume someone's behaviour or characteristics, thus leaving a margin of error that demands a balancing exercise that weighs the opportunities and risks of using such results. In this respect, legal scholars warn about the risks of a society that increasingly bases many decisions upon the outputs emanating from complex systems whose internal workings are not disclosed or easily understood (e.g., commonly called black boxes), especially in cases in which such decisions have a legally binding effect on subjects.[6]

---

[1] Moritz Büchi and others, 'The Chilling Effects of Algorithmic Profiling: Mapping the Issues' (2020) 36 *Computer Law & Security Review* 1–4.

[2] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (*Papers.ssrn.com*, 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829 accessed 3 July 2021; E. Fosch-Villaronga and others, 'A Little Bird Told Me Your Gender: Gender Inferences In Social Media' (2021) 58 *Information Processing & Management*.

[3] Colleen McCue, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis* (2nd edn, Butterworth-Heinemann 2014).

[4] Bart Custers, 'Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination' (2012) 3 *Privacy Observatory Magazine* 1–4.

[5] Bart Custers, 'Effects of unreliable group profiling by means of data mining' [International Conference on Discovery Science, 2003, Springer, Berlin, Heidelberg] 291–296.

[6] Pasquale Frank, *The Black Box Society* (Harvard University Press, 2015).

The EU General Data Protection Regulation (GDPR) establishes a framework to prevent these practices' risks and adverse consequences on data subjects through different instruments, including the right to receive meaningful information about the logic involved in such decision-making processes and the significance of the envisaged consequences of the ulterior decisions. The GDPR also protects data subjects against being subject to decisions producing legal or similarly significant effects based solely on automated processing under Article 22, thus limiting the cases in which automated decisions are permitted. Organizations and governments can only implement ADM processes concerning individuals if necessary to enter into or perform a contract between a data subject and a data controller, if ADM is authorized by Member State law, or if data subjects have given their explicit consent for such processing.

Despite these limitations, the GDPR falls short in providing enough safeguards to protect individuals from ADM. One shortcoming is the wording of a provision that states that ADM is permissible if 'necessary for entering into a contract',[7] which seems to imply that ADM processes can be conducted before (and therefore without) the data controller having a contract with the data subject. Another shortcoming are the inherent problems tied to consent, which may include the data subject not knowing or understanding ADM's consequences, even if the controller may have explained them in clear, understandable language.

In this chapter, we provide a general introduction to ADM and the legal safeguards EU data protection law puts in place to protect data subjects. After this short introduction, Section 2 briefly describes the automated decision-making system and how it works, including issues on the accuracy of ADM processes and their subsequent impact on data subjects. Section 3 describes how ADM is understood under the GDPR, examining the legal bases for the cases in which it is allowed. Section 4 discusses a number of issues related to the legal bases of ADM—most notably those concerning contract and consent—which include the ambiguity of Article 22 GDPR, the limits of consent within ADM, and the intricate interplay between contract and consent as legal bases. Section 5 provides conclusions.

2. AUTOMATED DECISION-MAKING PROCESSES

The widespread availability of data in many industries and their potential to make faster decisions is stimulating the use and proliferation of profiling techniques that support ulterior decision-making processes. The 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 person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[8]

This definition differs slightly from other legal scholars, such as Bosco et al., that defines profiling as 'a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that

---

7 Art 22(2)(a) GDPR.
8 Art 4(4) GDPR.

can subsequently be applied as a basis for decision-making';[9] or Custers, who defines it as a process in which characteristics are ascribed to individuals or groups of people, for instance by combining databases, predicting characteristics or clustering or categorizing people into different groups.[10] Clarke defines profiling as a process of constructing a series of information (i.e., profile), which is then applied to something or someone (i.e., individual or group) by techniques of data elaboration.[11]

ADM is defined in the GDPR as 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her';[12] this generally entails the 'processing of input data to produce a score or a choice that is used to support decisions such as prioritization, classification, association, and filtering'.[13] Hence, profiling focuses on analysing and predicting a person's characteristics, whereas ADM focuses on subsequent decisions based on such data and knowledge distilled from such processing.[14] These processes can be based on internal norms within an organization that govern a particular organization's business model or a legally binding norm. ADM processes 'make generally reliable (but subjective and not necessarily correct) decisions based upon complex rules that challenge or confound human capacities for action and comprehension'.[15]

Automated decision-making processes are based on data processing. In this chapter, we focus on personal data processing, which is within the scope of the GDPR, but ADM can also focus on the processing of non-personal data (for instance, for decision-making in industrial processes in which no data subjects are involved, or in case personal data is first anonymized before it is processed). In ADM, it is common that not only the decisions are automated, but also the data analytics. This is done via technologies such as *data mining*, in which algorithms are used to find patterns and relations in large dataset, *machine learning*, in which self-learning

---

[9] 'The PROtecting citizens' rights and Fighting ILlicit profilING (PROFILING) project' (Report 2020) https://www.academia.edu/20766799/PROFILING_Protecting_citizens_rights_fighting_illicit_profiling_with_Francesca_Bosco_Valeria_Ferraris_Daniel_Guagnin_Bert_Jaap_Koops_Bogdan_Manolea_accessed 3 July 2021.

[10] Bart Custers, 'Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self-Determination' (2012) 3 *Privacy Observatory Magazine* 1–4.

[11] Roger Clarke, 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance' (1993) 4 *JL & Inf. Sci.* 403.

[12] Art 22(1) GDPR.

[13] Hao-Fei Cheng and others, 'Explaining decision-making algorithms through UI: Strategies to help non-expert stakeholders' (In Proceedings of the 2019 CHI conference on human factors in computing systems, 2019, May) 1–12, p. 2. Another commentator defined it as 'the use of complex mathematical formulae to make commercial and social policy decisions'. Ari Ezra Waldman, 'Power, Process, and Automated Decision-Making' (2019) 88 *Fordham LR* 613, 613. A profile does not consist of raw data or mere observation. It is a mathematical model of facts or a reference to a group of points. It should be noted that many algorithmic models used for deriving profiles are opaque because it is difficult or impossible to determine how the resulting model was built and which correlations were considered. Therefore, the final step in profiling offers the possibility of making decisions based on the results that juxtapose the data of the individual with the generated profile. For more see: Hans Lammerant, and Paul De Hert, 'Predictive profiling and its legal limits: Effectiveness gone forever.', *Exploring the Boundaries of Big Data* [2016]. See also Matthias Spielkamp, 'Automating Society: Taking Stock of Automated Decision-Making in the EU' [2019] BertelsmannStiftung Studies 2019.

[14] Claude Castelluccia and Daniel Le Métayer, 'Understanding algorithmic decision-making: Opportunities and challenges' [2019] European Parliament.

[15] Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping The Debate' (2016) 3(2) *Big Data & Society* 1–21.

software extracts knowledge from data, and Artificial Intelligence (AI), in which autonomous digital (or cyber-physical) systems imitate cognitive functions so as to analyse data and make subsequent decisions.[16]

For automated discovery of patterns and relations in data there exist many different technologies. It is beyond the scope of this chapter to provide an overview, but one major category worth noting here is profiling. Profiles are often based on empirical data, such as test samples, which means that the results are usually statistical data, such as averages or probabilities. If these properties are valid for the group and for individuals as members of that group, though not for those individuals as such, this is referred to as *non-distributivity* or non-distributive properties.[17] On the other hand, when properties are valid for each individual member of a group as an individual, this is referred to as *distributivity* or distributive properties.

Given the statistical nature of most profiles upon which automated decisions are based, issues can arise with accuracy.[18] Furthermore, the complex nature of automated data analytics tools can yield transparency issues. This can particularly be the case when self-learning or autonomous systems are involved in data analytics and automated decision-making.

Inaccurate ADM processes affect users from different stands. One such example of data bias is 'statistical discrimination', which refers to making (un)educated guesses about an unobservable candidate characteristic, such as which applicants will perform well as employees. This has proven to be quite problematic. For instance, Amazon used an algorithm in its hiring process, and women candidates were more often devalued than men because the company had traditionally hired few women.[19] The algorithm concluded that being a woman was an undesirable characteristic for recruitment purposes. Thus, having a CV with the entry of being president of the 'women's chess club' was seen as a red-flag, giving the candidate more negative scores, while just generally being a member of a 'chess club' was seen as positive. Additionally, 'Women on Wikipedia tend to be more linked to men than vice versa. On a lexical level, we find that especially romantic relationships and family-related issues are much more frequently discussed on Wikipedia articles about women than men.'[20]

When the tools used to extract patterns and profiles from data are not transparent, it may be difficult for people to contest any decisions resulting from this, which may impede their freedom and autonomy. On top of that, if sensitive attributes, such as sexual orientation, ethnicity, religion, or trade union membership, are used for decision-making, this may result in discrimination, also from a legal perspective. For instance, in the EU, the GDPR provides

---

[16] Toon Calders and Bart Custers, 'What is Data Mining and How Does it Work?' in Bart Custers and others (eds), *Discrimination and Privacy in the Information Society* (Heidelberg: Springer 2013) 27–42.

[17] Anton Vedder, 'KDD: The Challenge to Individualism' (1999) 1 *Ethics and Information Technology* 275.

[18] Bart Custers, Effects of unreliable group profiling by means of data mining, [International Conference on Discovery Science, 2003, Springer, Berlin, Heidelberg] 291–296 and Gunter Grieser, Yuzuru Tanaka, and Akihiro Yamamoto, Lecture Notes in Artificial Intelligence [Proceedings of the 6th International Conference on Discovery Science (DS 2003) Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag] (Vol. 2843), 290–295.

[19] Miranda Bogen, 'All the Ways Hiring Algorithms Can Introduce Bias' (2019) *Harvard Business Review* https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias accessed 3 July 2021.

[20] Claudia WAGNER, and others, 'It's a man's Wikipedia? Assessing gender inequality in an online encyclopedia' [*Ninth international AAAI conference on web and social media* 2015] https://arxiv.org/pdf/1501.06307.pdf accessed 3 July 2021. *See* also Claudia Wagner and others, 'Women Through The Glass Ceiling: Gender Asymmetries In Wikipedia' (2016) 5 *EPJ Data Science* 1–24.

a framework for protection regarding the collection and processing of personal data, which also addresses discrimination issues in datasets.[21] However, scholars note that information about a person's gender, age, financial situation, geolocation, and online profiles are not sensitive data according to Article 9 of the GDPR, despite being grounds for discrimination.[22]

3. AUTOMATED DECISION-MAKING IN DATA PROTECTION LAW

The GDPR tries to prevent the risks involved in decision-making processes resulting from automated processing. However, though the focus is usually on the idea that ADM occurs *without human intervention*, ADM does not happen in a vacuum, but with humans intervening at different stages of the process:[23]

1. Humans delegate the decision to a machine or system.
2. Humans feed the system with data even though this can be an automatic procedure.
3. Once the decision is made, it may be interpreted by humans.

In this respect, the High-Level Expert Group on AI's 'Ethics Guidelines for Trustworthy AI' highlights that the development and use of AI, including ADM systems, must be fair on both a substantive and procedural level.[24] The substantive dimension implicates organizations' and governments' duty to increase societal fairness, that is, to ensure that individuals and groups are free from unfair bias and discriminatory decisions. Substantive fairness also refers to the utmost respect to the principle of proportionality between the means used to make a decision and the far-reaching implications of such a decision. The procedural dimension highlights the importance of contesting and challenging a decision made by ADM processes and providing an effective remedy against it.

The GDPR provision that most directly addresses ADM is Article 22 of the GDPR, which states:

> (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.

---

[21] Recital 71 GDPR.

[22] Sandra Wachter and Brent Mittelstadt, 'A Right To Reasonable Inferences: Re-Thinking Data Protection Law In The Age Of Big Data And AI' (*Papers.ssrn.com*, 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829 accessed 3 July 2021.

[23] Heike Felzmann and others, 'Transparency You Can Trust: Transparency Requirements For Artificial Intelligence Between Legal Norms And Contextual Concerns' (2019) 6 *Big Data & Society*.

[24] High-Level Expert Group on AI, HLEG on AI. Guidelines on Trustworthy AI. [2019] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai accessed 3 July 2021.

> (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.

This article was developed following the legacy of Article 15 of the Data Protection Directive (DPD)[25] and empowers data subjects by providing them with the option to invoke such a right. In line with this provision, the data subject had the right not to be subject to a decision producing legal effects or significantly affecting him or her if it was based solely on automated data processing.[26] The DPD already provided some examples of ADM, referring to evaluating 'certain personal aspects relating to [data subjects], such as [their] performance at work, creditworthiness, reliability, conduct, etc'.[27] In the GDPR, profiling represents a novelty in European data protection law,[28] expanding the application of data protection law to situations where certain personal aspects of the data subject are evaluated but there is no decision involved in such a process.[29]

Following the wording of Article 22, the GDPR provides for only three instances in which ADM can be applied to data subjects: when it is necessary for entering into, or the performance of, a contract between the data subject and a data controller; when it is authorized by Union or Member State law; or when it is based on the data subject's explicit consent.

Moreover, Article 22 of the GDPR requires controllers to implement suitable measures to safeguard data subjects' rights, freedoms, and legitimate interests in all cases.[30] Such a requirement contains the data subject's right to obtain human intervention on the data controller's part considering their point of view and to contest the decision,[31] as stated in Articles 13–15 of the

---

[25] Art 15 of the Directive 95/46/EC (DPD) of the European Parliament and of the Council of October 24, 1995, on the protection of individuals concerning the processing of personal data and on the free movement of such data, [1995] OJ L 281.

[26] The French Data Protection Act 1978 [Loi Informatique Et Libertés [Act on Information Technology, Data Files and Civil Liberties] [Act No.78–17, January 6. 1978] represents the sources for Art 15 DPD. Additionally, informational self-determination is grounded in Art 15, which means that an individual needs to have control over the data and information that is produced regarding him or her (the concept is recognized by the German Federal Constitutional Court -Bundesverfassungsgericht vom 15. Dezember 1983, BVerfG, Urteil Az. 1 BvR 209, 269, 362, 420, 440, 484/83).

[27] Art 15(1) DPD.

[28] The GDPR defines profiling in its Art 4(4) as:
> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

[29] A series of cases have had a large impact on the legislative process on the GDPR, including the Google Spain case (Case C-131/12, *Google Spain and Google* [2012] ECR EU: C:2014:317, para 37), the Digital Rights Ireland case (Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung and Others* [2012] ECR EU: C:2014:238, para 28), and the Schrems cases (Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [2014] ECR EU: C:2015:650, para 94).

[30] Art 22(3)(4) GDPR.

[31] Art 22(3) GDPR.

GDPR (dealing with the right to information and the right of access).[32] In that sense, the provisions in Articles 13 and 14 provide the data subject with the information necessary to ensure fair and transparent processing, while provisions in Article 15 require controllers to provide data subjects with information regarding the existence of automated decision-making (i.e., meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for the data subject). Note that the right to get an explanation of the decision reached is not legally mandated by the GDPR, as it is only mentioned in Recital 71 of the GDPR.[33] Because of this, the interpretation of the *right to explanation* in the GDPR has triggered a vivid debate among legal scholars.[34] Although opinions differ regarding the right to explanation, Recital 71 of the GDPR also attempts to address some of the risks of profiling. Beyond the GDPR, there is a need for additional regulatory tools that can facilitate the evaluation and revision of automated systems.[35]

Article 22(4) further states that where ADM utilizes sensitive data, there are only two possible legal bases: explicit consent and for reasons of substantial public interest.[36] In the following subsections, we expand upon the primary legal bases for ADM under the GDPR.

3.1 Contract

Contracts establish, confirm, and enforce an agreement between two or more parties. Today, traditional physically-written, paper-based contracts are often digital. In theory, and per the principle of autonomy and freedom of contract, the law should enforce any agreement that was freely made between different parties provided that it has no adverse effect on others.

---

[32] Arts 13(2)(f), 14(2)(g), and 15(1)(h) GDPR.

[33] Recital 71 GDPR. Here it should be noted that Wachter et al. called into doubt both the legal existence and the technical feasibility of the GDPR's *right to explanation* based in part on the fact that the GDPR does not legally mandate a *right to explanation*. However, the scholars have noted that the GDPR already legally mandates rights provided to the data subjects that include, at minimum, a *right to an explanation* of system functionality. 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' (20170 7 *International Data Privacy Law* 76–99.

[34] See, for instance, Bryce Goodman and Seth Flaxman, 'European Union Regulations On Algorithmic Decision-Making And A "Right To Explanation"' (20170 38 *AI Magazine*. Their published paper has pointed widespread attention to the technical and societal challenges of explaining machine learning algorithms' automated decisions and they suggest that the *right to explanation* could be satisfied relatively quickly. Moreover, Selbst and Powles have offered a positive concept of the *right to explanation* and they concluded that the right defined in the GDPR should be interpreted functionally and flexibly. See Andrew D Selbst and Julia Powles, 'Meaningful Information and The Right To Explanation' (2017) 7 *International Data Privacy Law* 233–242. Finally, in 2017 Malgieri and Comandé entered, and Malgieri continued the debate in 2019. According to them, the GDPR legally mandates either ex-ante or ex-post the *right to an explanation*. See 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*; and Gianclaudio Malgieri, 'Automated Decision-Making In The EU Member States: The Right To Explanation And Other 'Suitable Safeguards' In The National Legislations' (2019) 35 *Computer Law & Security Review*.

[35] For example, the rules stipulated by P2B Regulation, General Product Safety Directive, MIFID II Directive, and Medical Devices Directive, EU consumer law can be useful. For more see Maja Nisevic, The Right to an Explanation of Automated Decision-making Systems—Highlights of the Legal Landscape Referring to Explainable Ai: *Part 1 and 2* (2021) *C.T.L.R*.

[36] Art 22(4) and Art 9(2)(a) (g) GDPR.

In practice, these principles are put into question every day regarding digitally-based, data protection-related contracts. Users usually have a perceived sense of autonomy and freedom, often leading them into entering contracts that make them give away more of their data for more purposes, without fully understanding the consequences. Many times, the user may not be aware of the agreed terms and conditions, the extent to which they gave their data, or what their rights are.[37]

Despite this, a necessary part of conducting business in an algorithmic society is that data subjects often must provide detailed personal data, particularly when ADM is part of the requested service delivery. Otherwise, the service cannot be provided, and the contract cannot be performed. In such cases, the processing of personal data is of interest to both parties. However, the data controller's ability to rely on a contract as the legal basis for data processing in which ADM is involved does not exempt the controller from compliance with the other requirements stipulated in the GDPR.[38]

The formulation of Article 22(2) GDPR seems to suggest that data controllers can process personal data, create profiles, and make decisions upon these data to enter into contracts with data subjects, without having a previous agreement with the affected/interested data subject that would allow processing that data. This may be the case for applications for insurance, lines of credit, or even jobs, due to the large amount of data needed to be processed and the fact that it may 'potentially allow for greater consistency or fairness in the decision-making process'.[39] While giving information to enter into a contract seems logical from a contractual viewpoint, it is important to make a distinction between data collection and ADM processes. However, the GDPR is silent regarding the pre- and post-contractual relationship between data subjects and controllers, contract form, the type of obligation, and the contract's nature regarding ADM or profiling.

Although the Article 29 Working Party stressed the meaning of 'necessary for entering into... a contract',[40] from an examination of case law one must conclude that the concept of necessity has an independent meaning in European law, reflecting data protection law's objectives.[41] This entails that the data controller is able to show that ADM is in fact necessary; if there are less privacy-intrusive measures that are effective in achieving the same goal, then it cannot be considered 'necessary'.[42] In the context of Article 22 of the GDPR, this concept of 'necessary' applies to all the required conditions regarding contractual negotiations, the

---

[37] Bart Custers, 'Click Here To Consent Forever: Expiry Dates For Informed Consent' (2016) 3 *Big Data & Society*.

[38] Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR in the context of the provision of online services to data subjects, EDPB, [2019].

[39] Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 of Article 29 WP 29 [2017] pp. 13 and 23.

[40] The Article 29 Working Party has expressed views on the contractual necessity basis under the Data Protection Directive in its Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC [WP217] [2014], pp. 11, 16, 17, 18 and 55.

[41] Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland* [2008], ECR ECLI:EU:C:2008: 724, para 52. The CJEU stated in Huber that 'what is at issue is a concept [necessity] which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of [the Data Protection] Directive, as laid down in Article 1(1) thereof'.

[42] Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 of Article 29 WP 29 [2017] p. 23.

contract's formation, all the steps necessary to fulfil the contract, and the requirements needed to terminate the contract.

It appears that the controller is obliged to provide clear and undoubted intention regarding the creation of legal relations with the data subject, which is presented by a clear offer including specified lawful objects, such as personal data for the purpose of conducting ADM or profiling. In both cases, however, the data controller has to fulfil its contractual obligation in regard to providing meaningful information about the logic used, as well as the significance and envisaged effects of the processing of that data through ADM.[43] Therefore, a contract involving ADM also covers the exercise of legal claims that can arise from such a contract.

Different requirements determine a contract's validity for traditional paper-based agreements, which primarily include the intention to create legal relations, an offer and acceptance, consent, proper legal form, consideration, legal capacity, and a lawful object.[44]

Even though the GDPR is silent about the nature of contracts involving ADM, contracts must be valid under applicable laws regarding contracts and other rules that involve cross-functional responsibilities, including but not limited to consumer protection law and competition law.[45] However, it seems to suggest that such a contract should be perceived as a counter-performance contract because the data subject will be obliged to provide personal data in exchange for using the services. Usually, in such a contract, one of the clauses is a pre-formulated consent clause, which allows the organization to process personal data further, aiming to profile the data subject in the end.[46] As controllers primarily unilaterally draft contracts, it is likely that the cost of information per contract is higher for data subjects than for data controllers. Moreover, if data subjects want to negotiate a better deal regarding their privacy in a contract, they often lack the knowledge or the ability, or have little to gain in attempting to do so. Consequently, there is usually a power imbalance and asymmetric information between data subjects and data controllers.

The GDPR is silent about the relationship between contractual parties and contract termination because this is outside its scope. However, from a practical viewpoint, contract law interacts in one way or another with the GDPR as the data subject is a contractual party, and it is not possible to freely terminate the automated processing of personal data or ADM based on a contract. Similarly, the conditions under which contracting parties are legally able to termi-

---

[43] Arts 13–15 GDPR.

[44] For example, Italian Civil Code 1942 s 4 (Arts 1326–1338), or Zakon o obligacionim odnosima Republike Srbije, prečišćen tekst 2020 (Arts 27–78). *See* also Paolo Franceschetti , 'Accordo contrattuale AltalexPedia, voce agg' [14 March 2016] https://www.altalex.com/documents/altalexpedia/2016/03/04/accordo accessed 3 July 2021.

[45] This is also the opinion of EDPB, see Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR in the context of the provision of online services to data subjects, EDPB [2019] point 13 on p. 6.

[46] One example is a contract with a social network company. Social network services usually offer data subjects a contract when opening an account in exchange for personal data. For example, the Term and Services of Facebook state in point 2:

> How our services are funded: Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms you agree that we can show you ads that business and organizations pay us to promote on and off the Facebook Company Products. We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you.

Retrieved from: https://www.facebook.com/terms.php.

nate the contract are also not within the scope of the GDPR. The requirements for termination of a contract are instead within the ambit of national law. Still, data protection law is a primary benchmark, which entails that a contract concerning personal data for conducting ADM cannot be contrary to data protection law. Compared to a written contract, which usually contains contract termination conditions, a contract involving ADM arguably should also provide such conditions.

3.2 Member State Law

Following the formulation of Article 22(2)(b) GDPR, EU and Member State law can also form a legal basis for ADM,[47] with Recital 71 further stating that the EU and national authorities may allow ADM for a number of purposes. However, several of the societal domains that would be suitable for such a legal basis in national law are not within the scope of the GDPR. For instance, data processing (including automated decision-making) in domains like national security and law enforcement are regulated in separate legal frameworks, mostly on a national basis. Hence, automated data processing and automated decision-making for purposes like predictive policing, profiling terrorists or surveillance are beyond Article 22 GDPR.

Examples of uses that fall within the GDPR's scope include ADM 'for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller'.[48]

Concerning decisions based on profiling, Recital 73 further explains that EU and national laws can impose restrictions for reasons of public interest, for instance, to prevent or react to breaches of ethics for regulated professions or the keeping of public registers.[49] As a consequence, the GDPR clarifies that both EU and national laws can authorize ADM, subject to 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests'.[50] Ultimately, however, it is unclear to what extent ADM is permissible under this provision and how much leeway Member States have to enable ADM under national law.

---

[47] The EU Parliament researched the laws of member states that authorize ADM. See Answer from EU Parliament EN E-002800/2016 [30.6.2016].

[48] Recital 71 GDPR. See for instance the GDPR implementation act (Uitvoeringswet AVG) in the Netherlands, which clearly states that the legislator is to decide on ADM in the public sector and provide safeguards if ADM is used. Many systems in the public sector are covered by this, such as fraud detection in taxes and social benefits.

[49] Recital 73 GDPR.

[50] Art 22(2)(b) GDPR. Somewhat interestingly, this caveat is not present in the other legal bases for ADM, but a similar provision is applied to contract and explicit consent separately under Art 22(3).

3.3 Explicit Consent

Consent plays a crucial role as one of only six grounds that allow for the processing of personal data,[51] as detailed under Article 6 of the GDPR.[52] Here, it is worth noting that the GDPR distinguishes consent for the processing of personal data from consent for ADM and profiling. In this regard, the GDPR sets a special requirement for ADM in that consent for ADM must be 'explicit'.[53] However, the GDPR is silent about the exact meaning of the qualifier 'explicit',[54] and it only clarifies conditions for 'regular' consent.[55]

On the whole, the GDPR implemented a narrow interpretation of the concept of consent.[56] Following the requirements for valid consent, it should be kept in mind that there are some general limitations to using consent as a legal basis for data processing as the use of consent in the right context is crucial. Valid *regular* consent must be based on the conditions stated in Articles 4(11), 7, and 8 of the GDPR.

Valid consent requires an indication of wishes,[57] and the Court of Justice of the European Union (CJEU) has confirmed this on multiple occasions.[58] Moreover, the indication must be actively expressed.[59] Consequently, the notion of 'consent' includes the data subject's intent

---

[51] In fact, under the DPD, a number of countries gave consent a primary status in comparison to the other legal bases for processing personal data. For more see, Douwe Korff, 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments: Working Paper No.2: Data protection laws in the EU. The difficulties in meeting challenges posed by global social and technical developments' [2010], 69, https://www.altalex.com/documents/altalexpedia/2016/03/04/accordo accessed 3 July 2021.

[52] Art 4(11) GDPR stipulates that personal data may be processed based on 'freely given, specific, informed and unambiguous indication of the data subject's wishes'. Further, Art 7 outlines all the conditions required for valid consent.

[53] Art 22(2)(c) GDPR. Explicit consent is also a legal basis for the processing of special categories of personal data under Art 9(2)(a).

[54] This is a notion further explained by the Article 29 Working Party in Guidelines on consent under Regulation 2016/679 [2018]. According to these Guidelines, explicit consent 'means that the data subject must give an express statement of consent', such as a signed written statement, filling out an e-form, or using an electronic signature.

[55] In addition to the amended definition in Art 4(11), the GDPR provides additional guidance in Arts 7 and 8 and Recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main requirements for consent. Although explicit consent is also one of the exemptions to the prohibition on processing special categories of data according to Art 9, the GDPR does not define the meaning of explicit consent, contrary to the definition of regular consent for data processing. See, e.g., Opinion 15/2011 on the definition of consent for data processing WP29 [WP 187]. However, Article 29 Working Party in its Guidelines on consent under Regulation 2016/679 on p. 18, clearly distinguishes regular consent from explicit consent, including the term explicit.

[56] For instance, the definition of consent in Art 4(11) GDPR added the fact that the indication of wishes must be expressed 'by a statement or by a clear affirmative action', which was not present in the DPD. Additionally, and in contrast to the GDPR, the DPD was not very elaborate about certain aspects surrounding consent. The GDPR introduced the right to withdraw consent, a burden of proof for data controllers to prove individuals have given their consent, and special rules concerning consent by minors.

[57] Art 2(h) of the DPD and Art 4(11) of the GDPR.

[58] Case C-673/17 *Planet49* [2019] ECR ECLI:EU:C:2019:801, paras 52 and 61; Case C-61/19 *Orange România v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP) [2020] ECR ECLI:EU:C:2020:901, paras 35–36.

[59] Case C-673/17 *Planet49* [2019] ECR ECLI:EU:C:2019:801, paras 52 and 61; Case C-61/19 *Orange România* [2020] ECR ECLI:EU:C:2020:901, paras 35–36.

expressed through a declaration or a 'clear affirmative action', without which there can be no consent.[60]

Consent must also be unambiguous and freely given.[61] Here it is also important to clarify that valid consent exists only if it is informed consent.[62] This entails that the data subject should be informed of what exactly he or she is consenting to and, to some extent, made aware of the consequences such consent may have.[63] If the elements that constitute valid consent are unlikely to be present, or the data subject cannot decide because of social, psychological, or other pressure, the element of 'freely given' is not present.[64] Moreover, whenever the refusal of consent entails disadvantages for the data subject, consent cannot be assumed as freely given, and thus it would be invalid.[65]

As *explicit* consent is a legal basis for ADM, it is essential to discover the exact form of consent intended in Article 22(2)(c).[66] The European Data Protection Board (EDPB) has stressed that explicit consent requires a data controller's extra efforts regarding consent for ADM, including profiling.[67] As with regular consent, this entails that explicit consent includes, at a minimum, that the data subject gives a statement or clear affirmative action expressing their consent to ADM and profiling. Furthermore, data controllers bear the burden of proof that consent is given explicitly.

In the context of ADM, the meaning of explicit consent should be understood as consent that can constitute control and choice regarding whether to accept or decline ADM. This necessitates that explicit consent can be used as a tool that gives data subjects control over personal data concerning them which would be used for ADM operations. In that sense, a data controller should acquire consent from the data subject in writing or a similarly definitive

---

[60] A precursor to 'a statement or by a clear affirmative action' included in the definition of consent in Art 4(11) of the GDPR may perhaps be found in the CJEU's prior jurisprudence, where it was found that 'express consent' was required. Cases C-28/08 and T-194/04 *Bavarian Lager* [2010] ECR ECLI:EU:C:2010:378, para 77. (It should be noted that Art 2(h) of Regulation (EC) No. 45/2001 used the same definition of consent as that found in the DPD.)

[61] Recitals 32, 42, and 43 GDPR.

[62] Recital 42 GDPR and Case C-61/19 *Orange România* [2020] ECR ECLI:EU:C:2020:901, para 53, in which the Court stated that consent is not valid if a contract merely contains a clause stating that the data subject has been informed of the data collection. The consent is valid (and informed) only if the data controller has demonstrated:

> that the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts.

[63] Bart Custers and others, 'Consent and Privacy', in: A. Müller and P. Schaber (ed.), *The Routledge Handbook of the Ethics of Consent* (London: Routledge 2018), 247–258.

[64] Recitals 42 and 43 GDPR.

[65] Recital 42 GDPR.

[66] It should be noted that explicit consent also applies to consenting to the processing of special categories of personal data under Art 9(2)(a) GDPR.

[67] Guidelines 05/2020 on consent under Regulation 2016/679 [2020] EDPB, paras 91 and 92.

form of expressing consent.[68] Further, in cases of ADM, data controllers are encouraged to use a two-staged verification to confirm that explicit consent was validly provided.[69]

Moreover, the data controller is obliged to obtain separate (explicit) consent regarding ADM operations, and consent regarding other personal data processing.[70] In other words, consent must be separately obtained for each purpose the personal data is used for—different purposes cannot be bundled together.[71]

Therefore, when asking for consent for ADM, including profiling, a data controller has to obtain explicit consent based on Article 22 of the GDPR, in addition to the requirements for regular valid consent based on Articles 4, 7, and 8 of the GDPR. All in all, considering the differences between regular and explicit consent in the case of ADM, consent must be given under specific requirements and forms defined in the GDPR. In short, consent for ADM must be unambiguous and explicit, freely given, specific, and informed to be valid.

However, adding more formal elements to consent requirements does not *per se* improve individuals' data protection. In this sense, it seems useful to discuss whether consent should be considered an adequate legal basis for ADM in an increasingly algorithmic society, which will be examined in more detail below.

4. DISCUSSION

The complex technological nature of automated decision-making processes and the relatively general phrasing of the GDPR's legal provisions covering these practices raises many interpretation issues. This obviously leads to legal uncertainty. In this section, we discuss three major issues: the ambiguous phrasing of Article 22 of the GDPR, the limits of consent in ADM processes, and the complex interplay between contract and consent as a legal basis for ADM.

4.1 The Ambiguity of Article 22 of the GDPR

There are a number of potential problems regarding the ambiguity of Article 22(1) of the GDPR. First, it is questionable how to reveal the situations that could provoke data subjects to use the right stemming from Article 22(1) GDPR concerning 'legal or similarly significant effect'. Second, it is not clear whether the wording of Article 22(1) GDPR should be interpreted as a prohibition or a right for the data subject.[72] Third, it is not entirely clear whether

---

[68] Guidelines 05/2020 on consent under Regulation 2016/679 [2020] EDPB, paras 93 and 94. However, the EDPB noted that this may not be the only manner in which 'explicit' consent may be given. Other examples given include 'by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature' and perhaps even through 'oral statements'.

[69] Guidelines 05/2020 on consent under Regulation 2016/679 [2020] EDPB, para 98.

[70] For example, an explicit consent to cookies, without further explanation that the use of cookies could lead to profiling and without a button allowing the data subject to accept or reject such processing, should not constitute consent to an automated decision based on such profiling.

[71] Case C-673/17 *Planet49* [2019] ECR ECLI:EU:C:2019:801, para 58; Case C-61/19 *Orange România* [2020] ECR ECLI:EU:C:2020:901, para 38.

[72] See, e.g., Mendoza Isak, and Lee A. Bygrave, *The Right not to be Subject to Automated Decisions Based on Profiling* EU Internet Law (Springer, Cham 2017), 77–98.

automated decisions allow for any human involvement whatsoever. Here, we discuss these three issues.

While Article 22 of the GDPR endows the data subject with the right not to be subject to a decision based solely on automated processing, its framing, scope, and articulation are not very clear. From the article's wording, the possibility to exercise such a right seems to depend on the impact that a particular decision may have on the person. If the decision has no binding effect on the data subject and does not affect the data subject's legitimate interests, it seems that a decision based on an automated processing of personal data is considered to have a low impact on the data subject's life and, therefore, is allowed. Consequently, a low-impact decision will not provoke data subjects to exercise rights stipulated under Article 22 of the GDPR. However, when a decision is binding for individuals and affects their rights (e.g., by deciding whether a client should be awarded a line of credit, tax return or be employed), the law has to provide sufficient safeguards to protect this individual.[73] In that regard, Recital 71 of the GDPR provides some examples of decisions with a significant impact on the data subject,[74] e.g., the person's legal or contractual rights, financial circumstances, or ability to obtain essential or highly impactful goods or services, including health care, education, employment, and housing. However, there is not much guidance or examples focusing on other low-impact decisions.[75]

In this vein, while the Article 29 Working Party provides a bit of guidance through several other examples,[76] it is not clear what determines whether a decision is low or high risk for the data subject, leaving room for a multitude of approaches regarding the very same situation. For instance, automated gender recognition systems may infer the gender of users and may provide the basis for ulterior decisions, e.g., for marketing purposes. Given the accuracy of these systems, it may be the case that the system misgenders a person. While misgendering may have little impact for different populations, misgendering is particularly problematic for communities that have been historically discriminated against and for communities in which gender is a sensitive part of their identity.[77] Misgendering reinforces the idea that society does not consider a person's gender real, causing rejection, impacting self-esteem and confidence, the felt authenticity, and increasing one's perception of being socially stigmatized.[78] Thus,

---

[73] Maja Brkan, 'Do Algorithms Rule The World? Algorithmic Decision-Making And Data Protection In The Framework Of The GDPR And Beyond' (20190 27 *International Journal of Law and Information Technology*.

[74] Moreover, Recital 71 GDPR specifies that a decision may include a measure, and provides examples such as 'automatic refusal of an online credit application or e-recruiting practises without any human intervention'.

[75] For example, a speeding fine causes an obligation to pay the fine, or a building permit gives a new right to build something.

[76] Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 of Article 29 WP 29 [2017], p. 21.

[77] Kevin A. McLemore, 'Experiences With Misgendering: Identity Misclassification Of Transgender Spectrum Individuals' (2014) 14 *Self and Identity*.

J.Fergus, 'Twitter is guessing users' genders to sell ads and often getting it wrong, input' (2020) https://www.inputmag.com/tech/twitter-guesses-your-gender-to-serve-you-ads-relevant-tweets-wrong-misgendered accessed 3 July 2021.

[78] Os Keyes, 'The Misgendering Machines' (2018) 2 Proceedings of the ACM on Human-Computer Interaction.

although gender is not a special category of data, it may have an incredible effect on a large portion of the population.

Article 22(1) provides a great deal of discretion to decide on a case-by-case basis whether a particular scenario should be covered. In this respect, literature is rich in examples as to how 'innocent' or 'with good intention' inferential analytics that serve attention economics may reinforce existing biases that, although not explicit, can be very influential in exacerbating discrimination.[79] Similar to the stretching of the concept of personal data, the concept of how ADM may significantly impact data subjects will be fleshed out over time. This may be useful to prevent companies from defining reality. This means to say that companies often employ algorithms to automate certain processes in which they require certain definitions of the universe being automated. One example may be found in the start-up Jigsaw created *Perspective,* an AI-driven tool measuring toxicity levels of online content. In it, the company defined what 'toxic' meant in order to proceed to flag highly toxic content online. It turned out that the same tool would silence members of the LGBT community, including drag queens.[80]

A second issue is whether Article 22(1) should be interpreted as a right for the data subject and a prohibition for the data controller. If Article 22(1) is interpreted as a prohibition, data controllers would not be allowed to make automated decisions regarding data subjects unless there is a legal basis for ADM (i.e., a contract, authorization by Member State law, or explicit consent). Consequently, data subjects' protection against ADM seems to exist by default and would initially not require any action by the data subject. On the other hand, when Article 22 is interpreted as a right, the protection depends on the data subject's activity regarding the use of the right stipulated by Article 22(1).

As a consequence, the protection offered by the GDPR seems to rely heavily on the action or inaction of the data subject. Therefore, if Article 22(1) GDPR is considered as a right, data controllers would make automated decisions without additional requirements as long as the data subject would not disagree with the decision. However, there is debate whether Article 22(1) GDPR offers a prohibition or right.[81] Article 22 GDPR seems to imply that only ADM and profiling that fulfil the requirements stated under Article 22(2) and (3) are authorized by the GDPR. Therefore, it is more appropriate to understand Article 22(1) GDPR as a general prohibition for data controllers, albeit with exceptions.[82]

---

[79] Thomas H. Davenport and John C. Beck, 'The Attention Economy' (2001) *Ubiquity*; Aylin Caliskan, Joanna J. Bryson and Arvind Narayanan, 'Semantics Derived Automatically From Language Corpora Contain Human-Like Biases' (2017) 356 *Science* 183–186; Bart Custers, 'Profiling as Inferred Data. Amplifier Effects and Positive Feedback Loops' in Emre Bayamlıoğlu and others (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press, 2018), 112–115.

[80] Alessandra Gomes and others, 'Drag Queens and Artificial Intelligence: Should Computers Decide What is 'toxic' on the Internet?' *Internet Lab Blog*, https://www.internetlab.org.br/en/freedom-of-expression/drag-queens-and-artificial-intelligence-should-computers-decide-what-is-toxic-on-the-internet/ accessed 3 July 2021; Adam Poulsen, Eduard Fosch-Villaronga and Roger Andre Søraa, 'Queering Machines' (2020) 2 *Nature Machine Intelligence*.

[81] It is worth underlining that some commentators believe that by refusing the 'general prohibition' approach, some states will not comply with the GDPR; this in turn has practical consequences, for instance, in terms of the legality of cross-border data transfers. See Guido Noto La Diega, 'Against Algorithmic Decision-Making' (2018) *SSRN Electronic Journal*.

[82] The Article 29 Working Party stated that Article 22(1) 'establishes a general prohibition' of automated decision-making, meaning 'that individuals are automatically protected from the potential

A third confusing aspect of Article 22 of the GDPR is the extent to which humans can or cannot be involved given its heading, i.e., *automated* individual decision-making, combined with Article 22(1) which states that the provision is applicable to 'decisions based *solely* on automated processing'.[83] These references suggest that there is no human involved in ADM. However, as mentioned in Section 2, ADM does not happen in a vacuum where humans do not have any potential intervention. This is problematic because it gives the impression that the technology is not subjected to human responsibility,[84] which is not entirely true for at least three reasons. First, the delegation of decisions to a machine or system is made by humans, who define the scope of it and its framework.[85] Second, humans feed the system with the data even though this can be automated at a later point in time. Third, once the decision is made, it may be interpreted, applied, or used by humans.

Therefore, Article 22 GDPR is unclear about the extent of 'solely on automated processing', and whether the mere inclusion of formal human intervention in ADM processes may suffice to provide guidance.[86] Here, it is essential to clarify the role of humans in such processes because the provision could be interpreted as a permission for data controllers to incorporate humans into the decision-making process—even if such a human intervention has no substantive influence on the automated process—in order to justify that the process is no longer entirely automated, and thus that they have the right to process such data based on other legal bases which are less stringent. Nevertheless, according to the GDPR, data subjects have a right to insist on human intervention on the part of the controller as they have the right to express their point of view and contest the decision.[87] The GDPR has not specified that a data subject contesting the decision has to appeal to a human although it appears that there must be at least the possibility of human intervention and that, if requested by the data subject, a human should be tasked with reviewing the decision.[88]

From the wording in Article 22, it is also not clear whether the final decision itself must be fully automated. Article 22(1) explicitly mentions that decisions have to be based 'solely on automated processing'. Consequently, the fact that the final decision does not necessarily require full automation affects the level of human intervention allowed by the presumed protection under Article 22(1). In that sense, a decision must be based solely on the machine's processing or without human judgment in the ADM process as Article 22(1) mentions only 'automated processing'. As a consequence, formal human intervention without any substantive influence on the machine's process would be subject to the protection defined by Article 22(1). However, if a decision is produced with some level of direct human intervention, even

---

effects this type of processing may have'. See Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 [2017] Article WP 29, p. 19.

[83] Art 22(1) GDPR.

[84] Deborah G. Johnson, 'Technology With No Human Responsibility?' (2014) 127 *Journal of Business Ethics*.

[85] Cathy O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown, 2016).

[86] Human intervention in the ADM process is discussed in the literature. For example, Hildebrandt notes that 'the third pitfall concerns the fact that as soon as the decision is not automated due to a (routine) human intervention, the article no longer applies.' See Mireille Hildebrandt, 'Profiling And The Rule Of Law' (2008) 1 *Identity in the Information Society*.

[87] Art 22(3) GDPR.

[88] Dimitra Kamarinou, and others, 'Machine learning with Personal Data' [2016] Queen Mary School of Law Legal Studies Research Paper (247), 15.

when using machine output to draw a conclusion upon which a decision is made, it would not be subject to Article 22.[89]

To conclude, because Article 22 of the GDPR does not specify the nature of the decision, it implies broader possible interpretations regarding the level of human intervention.[90] While it is clear that Article 22 separates decisions 'based on automated processing' from other decisions, the decision must be directed to a particular data subject. It could be argued this means that Article 22 covers individual ADM only. This provokes strong arguments to move towards extending control by the data subject. A potential solution might be seen in Data Protection Impact Assessments (DPIAs) that could contain a document on how often a human decision-maker intervenes in decisions and whether his or her intervention changes the result of the decision in the end.[91] Since it is also clear that Article 22 encompasses ADM based on either personal data or sensitive data,[92] Article 22 provokes the application of all other core principles stipulated by the GDPR.[93]

4.2 The Limits of Consent within ADM

Consent has an essential role in EU data protection legislation as it represents one of the most critical grounds for legitimizing personal data processing under the GDPR. However, consent has its limits, also in regards to ADM. Informed consent is a mechanism that is intended to ensure that individuals make well-considered, conscious decisions for the processing of their personal data. People often overlook the information provided when consent is requested, in part because they are confronted with multiple consent decisions on a daily basis. Although the GDPR stresses the importance of providing information to the data subject about data processing, transparency relates to multiple concepts, fulfills many functions, and holds different promises revealing a tension between transparency as a normative ideal and its translation to practical application in many situations.[94] If ADM is involved, well-informed consent decisions are even more problematic due to the complexity of ADM's inner workings and the

---

[89] For example, the German so-called SCHUFA case [January 28 2014] VI ZR 156/13 (German Federal Court of Justice), para 34, concerning the use of automated credit-scoring systems. The court held that the credit-scoring system was outside the ambit of the German rules that transposed Art 15 DPD because the decision process's automated elements were pertaining to the preparation of evidence; the actual decision to provide credit was made by a person.

[90] This is the opinion of the Article 29 Working Party, see Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 [2017] Article 29 WP 29, pp. 8 and 21.

[91] Art 35 (33)(a) GDPR states that the Data Protection Impact Assessment is required in a case of an evaluation of personal aspects relating to natural persons which are based on ADM.

[92] Art 22(1), (2) and (3) GDPR refer to personal data, but Art 22(4) GDPR refers to sensitive data.

[93] The data controller has to respect principles as stated under Chapter 2 GDPR. The principles in the GDPR state that data must be processed lawfully, while the rules state that ADM and profiling are allowed under specified exceptions. Therefore, data controllers have to comply with the principles from Arts 5 and 6, and the rules from Article 22 GDPR. For example, see Joined cases C-465/00, C-138/01, and C-139/01. *Rechnungshof v Österreichischer Rundfunk and Others and Neukomm and Lauermann v Österreichischer Rundfunk* [2003] ECR ECLI:EU:C:2003:294, para 65 and case C-524/06, *Huber v Germany* [2008], ECR ECLI:EU:C:2008:724, para 48, in which the Court stated that processing activities are allowed but should comply with principles and the rules altogether.

[94] Heike Felzmann and others, 'Towards Transparency By Design For Artificial Intelligence' (2020) 26 *Science and Engineering Ethics*.

data controllers' difficulties in explaining the logic involved. As a result, it may translate into ineffective, meaningless consent.

Another limitation of consent is that it frames itself in relation to the processing of personal data known to the user, but not to the data that the user unconsciously reveals. In other words, while people generate some data explicitly, for instance, when posting messages on social media, additional information can be derived beyond people's knowledge and awareness.[95] For example, when posting a picture on Instagram, the picture itself reveals certain aspects, but all the metadata involved (such as when it was uploaded, to whom it was shared, who liked it, and who reshared it) reveal many more insights. Moreover, data processing technologies based on the information available from people who did consent and their conscious or unconscious sharing of data are suitable for predicting or inferring characteristics of people who refused to disclose personal data.[96]

Withdrawing consent is one of the potential forms of redress for data subjects if they change their minds after some time. However, this does not come without drawbacks. Revoking consent means revoking permission for the purpose under which personal data was initially collected, including for ADM, if applicable. This does not mean, however, that a data controller immediately needs to erase all data (the right to erasure in Art 17 of the GDPR would need to be invoked for that, and even this provision has its limitations).[97] Moreover, erasing data in automated environments is often complicated or even impossible, because the data may already have been shared with other data controllers and processors,[98] or because the data has already become part of the decision-making model through machine learning, as 'unlearning' this data can be very difficult.[99]

4.3 The Interplay between Contract and Consent as Legal Bases for ADM

According to some scholars, a contract could be reduced to a 'consent statement of the will, which is provided by two or more persons to produce a legal effect'.[100] Others describe it as 'a legal transaction in which one party provides another party with property performance, and the other party accepts it'.[101] However, several elements exist in a contract, including consent.[102]

---

[95] Bart Custers and Daniel Bachlechner, 'Advancing The EU Data Economy: Conditions For Realizing The Full Potential Of Data Reuse' (2017) 22 *Information Polity*.

[96] Jay Pil Choi, Doh-Shin Jeon and Byung-Cheol Kim, 'Privacy And Personal Data Collection With Information Externalities' (2019) 173 *Journal of Public Economics* 113–124.

[97] Arti 17 GDPR.

[98] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial Intelligence And The Right To Be Forgotten' (2018) 34 *Computer Law & Security Review* 304–313.

[99] Lucas Bourtoule, and others, 'Machine unlearning. arXiv preprint arXiv:1912.03817' [2019].

[100] Loza Bogdan, *Obilgaciono pravo* [2004], Sluzbeni glasnik Beograd, 93.

[101] Loza Bogdan, *Obilgaciono pravo* [2004], Sluzbeni glasnik Beograd, 93.

[102] For example, the Italian Civil Code requires, among other factors, agreement as a primary condition to form a valid contract. Art 1326 of the Italian Civil Code outlines that a contract is concluded at the moment when agreement exists between contractual parties. Agreement is a meeting of consent between the contractual parties. Therefore, consent of the contractual parties is essential for the validity of the contract. For more see: Italian Civil Code [Section 4] (Arts 1326–1338).

Regardless of consent being an essential element in a contract, Article 22(2) separates that notion from the concept generally espoused in the GDPR. Article 22(2) of the GDPR permits ADM and profiling either if the data subject consented explicitly or if it is necessary for entering into or performing a contract between the data subject and the controller. Consequently, it is an open question under Article 22(2) as to where the distinction between 'consent' for contract and 'explicit consent' lies or whether such a distinction even exists.

However, data subjects should take note of the legal basis used for ADM given the legal consequences that stem from contract formation. A contract is a legally binding agreement that establishes the rights and duties of the involved parties. Thus, a contract has an *inter partes* effect, whereas consent is a declaration of a person agreeing to something of one's own right, i.e., *sui iuris*. Consequently, the notions *entering into* and *performing a contract* imply a pre-formulated consent clause if the data subject is one of the contractual parties.

Although the difference between 'consent' for contract and 'explicit consent' may be crucial because the concepts have different requirements and legal consequences, the distinction between them, in terms of a written consent form, is likely to be very small—the only difference may be the counter-signing of it by the data controller in the case of a contract.

5. CONCLUSION

Organizations and governments worldwide process vast amounts of personal data and use it to support ulterior decision-making processes. Given the volume of information these organizations handle, these decisions are sometimes based solely on automated processes. However, ADM is a process based on complex rules that are poorly understood and yet they can adversely affect individuals' personal lives. Their inherent complexity and the speed with which decisions are being made challenge the transparency of the processes and their explainability, which only further frustrates the data subject's ability to adequately consent—whether explicitly or through a contract. Although the GDPR establishes the framework in which ADM can take place under Article 22, it leaves much to be desired.

This chapter examined the legal framework for automated decision-making under the GDPR. After introducing ADM processes and Article 22 of the GDPR, the legal bases for ADM—contract, Member State law, and explicit consent—were explored in more detail. Here, certain factors requiring more scrutiny were discussed, such as the meaning of 'necessary for entering into … a contract', which seems to imply that the ADM process can be carried out without a contract between the data controller and the data subject, which should not be the case. In this respect, the GDPR is silent regarding the pre- and post-contractual relationship between data subjects and controllers, contract form, the type of obligation, and the contract's nature regarding ADM or profiling. The meaning of 'explicit consent' (as opposed to 'regular' consent) was also delved into, and it was found that data controllers should acquire consent from the data subject in writing or a similarly definitive form of expressing consent on top of the requirements of regular consent; moreover, consent needs to be obtained separately for each purpose for which the personal data is used.

Further issues were identified and discussed, namely the ambiguous phrasing of Article 22 of the GDPR, the limits of consent in ADM processes, and the complex interplay between contract and consent as a legal basis for ADM.

The first of these relates to the wording of Article 22 which renders it difficult to interpret and implement. First, the ability to exercise the protections contained in Article 22 against an ADM process depends on the significant impact that a particular decision may have on a data subject. Second, questions remain about whether the provision should be interpreted as a right for data subjects or a prohibition against ADM for data controllers; it was found that it is most appropriate to view it as a general prohibition for data controllers, albeit with exceptions. Finally, the usage of 'based *solely* on automated processing' in Article 22(1) appears to disregard the fact that humans may still be involved in some parts of the decision-making process.

A second shortcoming with the provision is the inherent problems tied to consent. Data processing tools used, most notably knowledge discovery technologies, are evolving rapidly, allowing personal data to be aggregated, archived, and analysed across domains on a progressively wide-scale with significant impact and long-term consequences. Even if the controller may have explained them in clear, understandable language, data subjects may have a difficult time in understanding the logic involved within the ADM process and provide meaningful consent. Limitations in withdrawing consent within automated environments in an algorithmic society were also noted.

A final issue discussed in regard to Article 22 GDPR concerns the interplay between contract and consent as legal bases for ADM. Despite the fact that consent is a basic element in a contract, the GDPR distinguishes that notion from the legal basis of explicit consent for ADM. While the giving of explicit consent and agreeing to a contract may appear similar to a data subject in practice, there is in fact a large difference given the legal consequences that stem from contract formation.

ACKNOWLEDGEMENT

This research project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska -Curie grant agreement No 754345, under Region of Veneto Decree nr. 193 of 13/09/2016 and under Università degli Studi di Verona.