The Italian Law Journal's Book Series
Cultural Asset - 5

7423054230

Automation has proven to be capable of producing extremely positive results in terms of increased efficiency and speed in decision-making, but it often conceals the risk of discrimination. Discriminatory practices may affect new types of groups, identified through inferential association, that do not correspond to historically protected grounds. Where the anti-discrimination law does not reach, the data protection law may. Based on an analytical examination of the legal provisions and a comparison with the positions of legal scholars and the European Court of Justice case-law, the study examines whether the GDPR provides effective tools to counter algorithmic discriminations based on unprotected attributes.

Alfio Guido Grasso is a researcher at the University of Catania, where he lectures. He has taught at the Catholic University of Milan. He has carried out visiting research at the Universities of Coimbra, Manchester and Humboldt. He was visiting scholar at the Weizenbaum Institute for the Networked Society in Berlin. He is the author of *Maternità surrogata altruistica e tecniche di costituzione dello status* and several essays on private law topics.

Alfio Guido Grasso
GDPR Feasibility and Non-Statutory Algorithmic Discrimination
ESI

Questo volume, sprovvisto del talloncino a fronte, è da considerarsi copia saggio gratuito esente da IVA (art. 2, c. 3, lett. d, DPR 633/1972)

ISBN 978-88-495-5249-2

€ 25,00

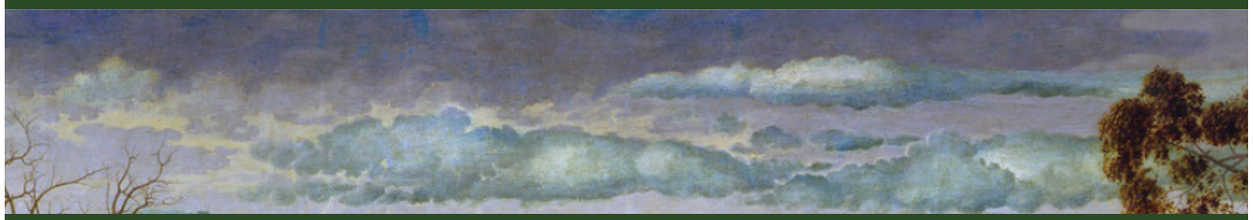
9 788849 552492

The Italian Law Journal
Book Series

Cultural Asset
5

Alfio Guido Grasso

GDPR Feasibility and Algorithmic Non-Statutory Discrimination



Edizioni Scientifiche Italiane

The Italian Law Journal's Book Series
Cultural Asset

5

General Editors

Camilla Crea (Università degli Studi del Sannio)
Andrea Federico (Università degli Studi di Salerno)
Pasquale Femia (Università degli Studi di Salerno)
Giovanni Perlingieri (Università degli Studi Roma La Sapienza)

Nella stessa collana:

1. L. Coppo, *Contract As a Tool for Getting-To-Yes: A Civil Law Perspective*, 2018
2. *Waste Life, Law and Management*, Erika Giorgini and Marco Giuliani (*edited by*), 2021
3. E. Maio, *Civil Liability and Autonomous Vehicles*, 2022
4. S. Serravalle, *The Italian implementation of the Copyright Directive. New models of collective rights management and limitations for rightolders*, 2022

GDPR Feasibility and Algorithmic Non-Statutory Discrimination

by Alfio Guido Grasso

Edizioni Scientifiche Italiane

Published with funds from the Law Department of the University of Catania.

Acknowledge financial support from: PNRR MUR project PE0000013-FAIR.

Programma di ricerca di Ateneo UNICT 2020-22 linea 2.

Thanks also to the German Federal Ministry of Education and Research (BMBF) for the support. Grant number: 16DII112 - "German Internet Institute"/„Deutsches Internet-Institut".

Grasso, Alfio Guido
GDPR Feasibility and Algorithmic Non-Statutory Discrimination
The Italian Law Journal's Book Series - Cultural Asset, 5
Napoli: Edizioni Scientifiche Italiane, 2023
pp. 136; 24 cm
ISBN 978-88-495-5249-2

© 2023 by Edizioni Scientifiche Italiane s.p.a.
80121 Napoli, via Chiatamone 7

Internet: www.edizioniesi.it
E-mail: info@edizioniesi.it

I diritti di traduzione, riproduzione e adattamento totale o parziale e con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche) sono riservati per tutti i Paesi.

Fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, comma 4 della legge 22 aprile 1941, n. 633 ovvero dall'accordo stipulato tra SIAE, AIE, SNS e CNA, CONFARTIGIANATO, CASA, CLAAI, CONFCOMMERCIO, CONFESERCENTI il 18 dicembre 2000.

Introduction

Especially since the COVID-19 pandemic,[1] more and more automated systems are involved in the formulation of decisions which have a significant impact on individual and collective life, and which increasingly affect key public functions, such as the administration of justice, the credit system or access to social services.[2] In all these areas, automated decision-making, especially when combined with the computing power of artificial intelligence, have proven to be able to produce extremely positive results – especially in terms of greater efficiency and speed in decision-making, which can also be reflected in a reduction in inequalities.[3]

[1] See M.E. Kaminski and J.M. Urban, 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189-218 (2019), recounting a number of cases where, instead of traditional examinations that were unsuitable because of the pandemic, assessment algorithms were used for university admission. The unexpectedly low results of some students sparked outrage, suggesting that those from historically poor performing schools may have been disadvantaged, thereby disproportionately harming students from historically marginalized groups.

[2] For a general overview see, among others, the recent collective works on this topic by W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor and G. De Gregorio eds, 'Constitutional Challenges in the Algorithmic Society' (Cambridge: Cambridge University Press, 2021); U. Ruffolo ed, 'Intelligenza artificiale. Il diritto, i diritti, l'etica' (Milano: Giuffrè, 2020); G. Alpa ed, 'Diritto e intelligenza artificiale' (Pisa: Pacini Editore, 2020); E. Gabrielli and U. Ruffolo eds, 'Intelligenza artificiale e diritto' *Giurisprudenza italiana*, Sezione Monografica, 1657 (2019); S. Lohsse, R. Schulze and D. Staudenmayer eds, 'Liability for Artificial Intelligence and the Internet of Things' (München-Oxford: Bloomsbury Publishing, 2019); W. Barfield and U. Pagallo, 'Research Handbook on the Law of Artificial Intelligence' (Cheltenham: Edward Elgar Publishing, 2018); J.A. Kroll, J. Huey, S. Barocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson and H. Yu, 'Accountable Algorithms' 165, *University of Pennsylvania Law Review*, 633-705 (2017).

[3] Consider this example.

One company identified the distance between home and workplace as a strong predictor of job retention, yet decided not to use this factor in its hiring algorithm because it understood that housing patterns are correlated with race and relying on that correlation could have led to discrimination: see D. Volz, 'Silicon Valley Thinks It Has the Answer to Its Diversity Problem' ATLANTIC (Sept. 26, 2014), available at www.theatlantic.com/politics/archive/2014/09/silicon-valleythinks-it-has-the-answer-to-its-diversity-

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

However, in many other cases, the use of decision-making algorithms has proven to be an enhancer and exacerbating factor of discrimination.

The most common reason is due to the presence of bias, which in itself leads to systematic errors that influence judgment and decisions.[4] These distortions or false representations of reality may also affect computer systems, which consistently and unfairly discriminate against certain individuals or groups of individuals in favor of others, denying opportunity or generating unwanted results for unreasonable or inappropriate reasons. All the main acts governing the use of artificial intelligence, including the latest Proposal for a Regulation of the European Commission,[5] warn against the risk of bias.[6]

problem/431334/ (last access 5 April 2023). A beneficial effect that could go even further if, "in addition to eliminating the factor as a basis for decision-making, an employer might use the information to examine whether its workplace practices make it more difficult for employees who travel long distances to succeed. A firm committed to a diverse workforce but located in a city with a segregated housing market might consider policies like flex-time or benefits like public transit passes in order to relieve a commuting burden that falls more heavily on already disadvantaged groups": see P. Kim, 'Data-Driven Discrimination at Work' 58 *William & Mary Law Review*, 3, 857-936 (2017).

[4] See European Union Agency for Fundamental Rights, 'Bias in Algorithms artificial intelligence and discrimination' (Luxembourg: Publications Office of the European Union, 2022).

[5] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Brussels 21.04.2021, COM(2021) 206 final 2021/0106 (COD).

[6] On the risk of algorithmic discrimination and the latest European proposals for a regulation on artificial intelligence, see A. D'Adda, 'Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo' *Rivista di diritto civile*, 5, 805-837 (2022); N. Eder, 'Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling', in M. Ebers and M. Cantero Gamito eds, *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges*, (Cham: Springer, 2021), I, 23-47; G. Di Rosa, 'Quali regole per i sistemi automatizzati "intelligenti"?' *Rivista di diritto civile*, 5, 823-853 (2021); P. Stanzione, 'Data Protection and vulnerability' *European Journal of Privacy Law & Technologies*, 2, 9-14 (2020); S. Amato, 'Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie' (Torino: Giappichelli, 2020), 60; U. Salanitro, 'Intelligenza artificiale e responsabilità: la strategia della Commissione europea' *Rivista di diritto civile*, 6, 1246-1276 (2020); G. Gitti, 'Dall'autonomia regolamentare e autoritativa alla automazione della decisione robotica', *Tecnologie e diritto*, 1, 113-127 (2020); L. Avitabile, 'Il diritto davanti all'algoritmo' *Rivista italiana per le scienze giuridiche,* 8, 315-327 (2017).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Biases may belong – first and foremost – to the designers, who may influence the algorithm setting through the inclusion or exclusion of characters that identify or refer to a protected category. More commonly, however, discriminatory effects arise from variables that are introduced into the algorithm because of the goal it is intended to pursue, which can give rise to forms of indirect discrimination. In this case, the same – apparently neutral – treatment afforded to individuals in different situations place some people in a position of particular disadvantage over others.[7] In contrast, it is quite rare that discrimination is direct, which could be verified if the decision maker explicitly used membership in a protected group as input for the model and assigned it lower scores.[8] However, since developers strive for accuracy, cases of direct discrimination will be quite rare, because directly including discrimination in an algorithmic model is likely to reduce its predictive value, which is an important disincentive.[9]

Yet discriminatory effects can also derive from the contents of the data set used to "feed" the machine learning system. Algorithms, in fact, work according to the garbage in/garbage out logic, so incongruous, inaccurate or outdated data can produce unreliable decision-making results. There are many examples of this.

One of the best-known affairs is the one related to the use of COMPAS, a software mainly trained by a database of judicial precedents able to predict the risk of recidivism and social danger of the accused and used to decide on the extent and manner of the execution

[7] Returning to the above example, if in the programming of an algorithm used for the recruitment of staff the notion of a "good" employee is defined by the criterion of punctuality, this may result in a systematic penalization of all those who live in the suburbs and therefore take longer to reach the company's headquarters every day. And since in certain contexts the circumstance of living in the suburbs is a variable closely related to the ethnic origins and the most disadvantaged social conditions, such a formally "neutral" criterion could be reflected in the detriment of already disadvantaged groups: see G. Resta, 'Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza' *Politica del diritto*, 2, 199-236 (2019), 217.

[8] See P. Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' 55 *Common Market Law Review*, 4, 1143-1185 (2018).

[9] In addition, there is usually awareness of the legal obligations not to directly treat protected groups differently. See 'EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination', in U. Bernitz, X. Groussot, J. Paju and S.A. De Vries eds, *General principles of EU law and the EU digital order* (Alphen aan den Rijn: Kluwer Law International, 2020), 151-182.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

of criminal penalties. The subsequent verification of the correctness of the forecasts showed that the judicial precedents used, unfavorable to the black convicts, had induced the system to underestimate the probability of recidivism of the white convicts and to overestimate that of the black convicts.[10]

Another example, related to security and crime prosecution, may be that of a facial recognition system that has been trained on a sample that includes few members of a certain ethnic group: there will be more recognition fails with respect to that group, which may lead to serious disadvantages (such as the likelihood of being wrongly charged).[11]

Frequently the unfair decision lies in the past because the algorithm, to elaborate predictions for the future, bases its knowledge on existing empirical events.[12] An example of this may be the Amazon case.

In 2014, Amazon built an artificial intelligence system with the aim of evaluating the candidates' resumes as quickly as possible in order to select the highest-level talents. The program scored candidates with one to five stars, just as customers do when buying any product on the company's website.[13] The artificial intelligence application used by the company was based on files with profiles of job seekers from the last 10 years, most of whom were men. Hence, AI learned that men were preferable and began to discriminate against women, penalizing resumes that contained the word "woman".[14] This software inclination to project the circumstances of the past into the future risks perpetuating privileged situations and thus excluding persons

[10] See B. De Felippe Reis and V.M. Caxambu Graminho, 'A inteligência artificial no recrutamento de trabalhadores: o caso amazon analisado sob a ótica dos direitos fundamentais' *XVI Seminário Internacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea*, (2019), available at https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/19599/1192612314 (last access 5 April 2023); I. Ferrari, D. Becker and E.N. Wolkart, 'Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos' 107 *Revista dos Tribunais, São Paulo*, 995, 635-655 (2018).

[11] See F. Lagioia and G. Sartor, 'Il sistema COMPAS: algoritmi, previsioni, iniquità', in U. Ruffolo ed, *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (Giappichelli: Torino, 2021), 226-243, 228.

[12] See T. Zarsky, 'Transparent predictions' *University of Illinois Law Review*, 1503-1570 (2013), 1505.

[13] The case gained international attention after the company admitted that the system had promoted gender discrimination against female candidates for the role of software developer and other technical positions in the company.

[14] After becoming aware of the problem, the company decided to abandon the project.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

belonging to certain social groups from access to relevant employment positions, access to care, to the credit system, and so on.[15]

The propensity to crystallize a certain state of the world in the prognostic process goes along with the classification of people into social groups, generalizing the assumption that people with such characteristics are more likely to act in a certain way or possess specific qualities.[16] But generalizing can lead to discriminating those people who do not adapt to the characteristics of the general group.[17] The decision taken statistically, albeit by a perfectly implementing algorithm, may not be correct, especially in relation to the individual case, since statistics provide more reliable information on an overall rather than on a local effect.[18]

Many more examples could be given, and others will be illustrated in the course of the discussion, but at the moment it is more important to focus on the limits that EU anti-discrimination law encounters when applied to algorithmic decision-making. European anti-discrimination legislation, in fact, frequently is totally inapplicable to decisions taken by automated systems, and, even when it is, it requires an expansive and benevolent interpretation that is not always consistent with the normative logic behind it.[19] European anti-discrimination legislation was conceived for a different context and for different needs from those posed by automated devices.[20]

[15] See D. Lyon, 'Surveillance as social sorting: privacy, risk, and digital discrimination' (Routledge: New York, 2003), 27.

[16] See G. Britz, 'Freie enfaltung durch selbstdarstellung' (Tübingen: Mohr Siebeck, 2007), 134.

[17] See S. Barocas and A. Selbst, 'Big Data's Disparate Impact' 104 *California Law Review*, 3, 671-732 (2016), 684; J. Lerman, 'Big data and its exclusions' 66 *Stanford Law Review Online*, 55-63 (2013); K. Crawford, 'Think Again: Big Data' *Foreign Pol'y* (May 10, 2013), available at https://foreignpolicy.com/2013/05/10/think-again-big-data/ (last access 5 April 2023).

[18] Statistics based on probability theory, by definition, can never lead to certain conclusions, but only to likely ones: see S. Tommasi, 'Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo' 27 *Revista de Direito Brasileira*, 10, 112-129 (2020), 115. Statistic outcomes can legitimize more or less strong doubts – and this is certainly a useful function – but they can never quash them definitively. They can provide no "element of certainty", but only "elements of suspicion": see C. Gini, 'I pericoli della Statistica' (Roma, 1939), 133, available at *http://blog.petiteplaisance.it/wp-content/uploads/2018/01/04-Corrado-Gini-I-pericoli-della-statistica_08.pdf* (last access 13 June 2022).

[19] See P. Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' 55 *Common Market Law Review*, 4, 1143-1185 (2018), 4.

[20] See J. Gerards and R. Xenidis, 'Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law' (Luxembourg:

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Not all the inequalities related to the development of artificial intelligence can be legally qualified as discrimination, because many examples of unfairness are outside the scope of any current non-discrimination law "which tends to focus on a specific 'bad actor' and individual victims".[21] Apart from the hypothesis of discriminatory intent hidden behind a distorted data model (for example, an employer against his employee),[22] the algorithmic discrimination is not driven indeed by any intentionality and it does not target a specific person but an entire category: it is a systematic, large-scale discrimination.

Moreover, and more radically, the European legislator decided to repress only certain manifestations and certain forms of discrimination, choosing to regulate the phenomenon only in some precise objective

Publications Office of the European Union, 2021); P. Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' 55 *Common Market Law Review*, 4, 1143-1185 (2018); R. Xenidis and L. Senden, 'EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination', in U. Bernitz, X. Groussot, J. Paju and S.A. De Vries eds, *General principles of EU law and the EU digital order* (Alphen aan den Rijn: Kluwer Law International, 2020), 151-182; F.J. Zuiderveen Borgesius, 'Discrimination, artificial intelligence, and algorithmic' (Strasbourg: Published by the Directorate General of Democracy of the Council of Europe, 2018).

[21] See P. Kim, 'Data-Driven Discrimination at Work' 58 *William & Mary Law Review*, 3, 857-936 (2017), 865. On the limits of anti-discrimination law more broadly see V. Barba, 'Principio di eguaglianza e tutela dei contraenti', in M. Cavallaro, F. Romeo, E. Bivona and M. Lazzara eds, *Sui mobili confini del diritto. Scritti in onore di Massimo Paradiso*, II, 333-383; G. Donadio, 'Responsabilità da violazione del divieto di discriminazione', in E. Navarretta, *Codice della responsabilità civile* (Milano: Giuffrè, 2021), 2509-2520; B. Checchini, 'Discriminazione contrattuale e dignità della persona' (Torino: Giappichelli, 2019), 155; G. Carapezza Figlia, 'Il divieto di discriminazione quale limite all'autonomia contrattuale' *Rivista di diritto civile*, 6, 1387-1418 (2015); E. Navarretta, "Principio di uguaglianza, principio di non discriminazione e contratto' *Rivista di diritto civile*, 3, 547-566 (2014); D. Maffeis, 'Discriminazione (diritto privato)' *Enciclopedia del Diritto* (Milano: Giuffrè, 2011), Annali, IV, 490-510; L. Sitzia, 'Pari dignità e discriminazione' (Napoli: Jovene Editore, 2011), 177; A. Gentili, 'Il principio di non discriminazione nei rapporti civili' 27 *Rivista critica di diritto privato*, 2, 207-231 (2009); D. La Rocca, 'Le discriminazioni nei contratti di scambio di beni e servizi', in M. Barbera ed, *Il nuovo diritto antidiscriminatorio. Il quadro comunitario e nazionale* (Milano: Giuffré, 2007), 289-341; P. Morozzo della Rocca ed, 'Principio di uguaglianza e divieto di compiere atti discriminatori' (Napoli: Edizioni Scientifiche Italiane, 2002); M. Bell, 'Anti-discrimination law and the European Union' (Oxford: Oxford University Press, 2002).

[22] It is unlikely that the employer would use a data model (whose errors he or she knows) intentionally against the employee he or she wants to discriminate. It is no less absurd to suppose that an employer would order the provision of a model that is specifically biased to discriminate against certain employees.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

and subjective areas. [23] But the point is that automatic decisions often target characteristics that are not protected by law. This is why if, in some cases, these effects can theoretically be repressed on the basis of the rules enacted by European law to safeguard the individual in a wide range of areas (from employment to social security, from healthcare to access to goods and services), against discrimination based on a specific protected ground (religion, gender, ethnicity, political belief, etc.). [24] In many other instances, a similar protection cannot be granted, since algorithmic decisions give decisive relevance to motives that are not sheltered by law, as they are generally not considered to be sensitive attributes.

Algorithmic decisions are often based on characteristics that have never been the object of persecution throughout human history and, consequently, the legislature has never felt the need to protect these groups, as no moral judgment or disadvantaged social *status* has ever been associated with them. For example, less favourable treatment was given to people who own dogs, video gamer,[25] or people who are keen

[23] E. Consiglio, 'Che cos'è la discriminazione? Un'introduzione teorica al diritto antidiscriminatorio' (Giappichelli: Torino, 2020), 21.

[24] Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin ("Racial Equality Directive"). Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation ("Employment Equality Directive"). Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation ("Equal Treatment Directive") (Recast). Directive 79/7/EEC of 19 December 1978 on the progressive implementation of the principle of equal treatment for men and women in matters of social security. Directive 92/85/EEC of 19 October 1992 on the introduction of measures to encourage improvements in the safety and health at work of pregnant workers and workers who have recently given birth or are breastfeeding. Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services ("Directive on equal treatment between men and women in the access to and supply of goods and services"). Directive 2010/18/EU of 8 March 2010 implementing the revised Framework Agreement on parental leave concluded by BUSINESSEUROPE, EAPME, CEEP and ETUC and repealing Directive 96/34/EC. Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010 on the application of the principle of equal treatment between men and women engaged in an activity in a self-employed capacity and repealing Directive 86/613/EEC. Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, replacing Council Framework Decision 2002/629/JHA.

[25] See N. Kobie, 'The Complicated Truth About China's Social Credit System',

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

on winter activities, or people who use Facebook a lot, [26] or who are identified as "sad teenagers". [27] But groups such as "dog owners" or winter sports fans are not protected by non-discrimination laws.

However, risk factors are constantly evolving, depending on the evolution of social consciousness and the reaction of a given community under certain circumstances. Consequently, specific regulatory applications to certain risk factors, such as race or gender equality, could be considered exemplifications of discipline or facilitation of discrimination proof. Yet, regulation limited to one or more risk factors would not constitute a restriction on the recognition of other risk factors or the extension of coverage of discrimination to other areas. [28]

Indications to this effect can be drawn from Article 21 of the Charter of Fundamental Rights of the European Union and Article 14 of the European Convention on Human Rights, which contain a very large list of categories on the basis of which discrimination is prohibited and both include unclosed expressions that could allow these lists to be considered as non-exhaustive. [29] Legal scholars deem the list to be an open one, susceptible to expansion by case law and European

WIRED UK (June 7, 2019), https://www.wired.co.uk/article/china-social-credit-system-explained (last access 2 April 2023), where reports about the fact that being labelled as a game player can lower one's Chinese social credit score.

[26] See Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability B-2–B-6 (2014).

[27] M. Reilly 'Is Facebook Targeting Ads at Sad Teens?' *MIT Technology Review* (2017), https://www.technologyreview.com/s/604307/is-facebook-targeting-ads-at-sad-teens/ (last access 5 April 2023).

[28] See V. Barba, 'Principio di eguaglianza e tutela dei contraenti', in M. Cavallaro, F. Romeo, E. Bivona and M. Lazzara eds, *Sui mobili confini del diritto. Scritti in onore di Massimo Paradiso*, II, 333-383, 344.

[29] Article 21 of the Charter of Fundamental Rights of the European Union states: "1. **Any** discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited". Article 14 of European Convention on Human Rights states: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or **other status**.". (emphasis added).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

secondary legislation.[30] Although the Court of Justice of the European Union (ECJ) ruled that it is not in its power to create new protected groups,[31] by leveraging these textual openings the risk factors could also encompass new ones. Consequently – and thus, for example, associating the possession of a dog with a protected attribute – any decision based directly on this attribute could already be classified as direct discrimination, and thus the related differentiation safeguarded as a consequence.

Looking further, however, this approach runs into obstacles, especially in contractual matters. When confronted with the principle of freedom of contract, the principle of non-discrimination must find specific normative applications to warrant the counterparty's obligation to treat others fairly.[32] Anti-discrimination rules require explicit substantive provisions because they are invariably mandatory, given their *raison d'être*. However, precisely because of their mandatory nature, they cannot be imposed without an explicit rule providing for it, since they produce a significant restriction on the freedom to conduct business and trade (the consideration of which is also behind the General Data Protection Regulation).

If dog ownership were not recognised as a protected attribute, the targeted individuals could still invoke indirect discrimination to obtain protection. In this case, it must be demonstrated by the claimant that a significant enough percentage of group members are likely to be members of a protected group (which would receive disproportionately negative treatment), when compared to others in a similar situation. And the applicant himself must be a member of the disadvantaged protected group.[33] However, apart from the technical difficulties of detecting the proxy power of dog ownership, it may be the case that this category does not sufficiently match a protected group, where disproportionate means that about 80-90% of the group must be disadvantaged.[34] The Court of Justice of the European Union

[30] N. Parisi and G. Urso, 'I principi di eguaglianza e di non discriminazione nell'ordinamento dell'Unione europea' *Osservatorio sul rispetto dei diritti fondamentali in Europa*, available at www.europeanrights.eu, 24 (2011), 9.

[31] See, e.g., Case C-303/06, Coleman v. Law, 2008 E.C.R. I-415, ¶ 46.

[32] See D. Maffeis, 'Il contraente e la disparità di trattamento delle controparti' *Rivista di diritto privato*, 281-312 (2006), 281.

[33] See S. Wachter, 'Affinity profiling and discrimination by association in online behavioral advertising' 35 *Berkeley Technology Law Journal*, 367-430 (2020), 372.

[34] See, e.g., Case C-443/15, Parris v. Trinity College Dublin, ECLI:EU:C:2016:897, ¶ 80.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

(ECJ), in relation to the proportionality threshold, explained that a measure "taken in isolation" must produce the disproportionate effect for one of the protected grounds.[35] It may therefore be the case that the profile of "dog owners" is not homogeneous enough to meet this requirement and that they do not have such a shared and compact group identity to fulfil this requirement.

In the face of this ineffectiveness of anti-discrimination laws, other paths have been suggested to be explored to address the challenges of algorithmic decision-making, in order not to leave a regulatory vacuum in an area potentially so prone to discrimination.[36] An alternative to non-discrimination laws has been identified in the algorithmic decision-making regime contained in Article 22 of the GDPR, entitled "Automated individual decision-making, including profiling".[37]

The text of the provision reads as follows:

"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. Decisions

[35] One may think that dog ownership is used as a statistical indicator or proxy from which other characteristics or traits of the person, protected in this case, such as sexual gender, age or ethnicity, are derived. But the ownership of a dog is a clear example of a case that cuts across all social, cultural, income, ethnic groups, etc. in a proportionate way, or at any rate the differences (which there will be) are far from the percentage value required by the ECJ.

[36] See R. Gellert, K. De Vries, P. De Hert and S. Gutwirth, 'A Comparative Analysis of Anti-Discrimination and Data Protection Legislations', in B. Custers, T. Calders, B. Schermer and T. Zarsky eds, *Discrimination and Privacy in the Information Society* (Cham: Springer, 2013), 61.

[37] See P. Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' 55 *Common Market Law Review*, 4, 1143-1185 (2018), 25.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

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".

In this unique provision,[38] which, in some ways, seems to represent an independent island from (and in) the rest of the Regulation,[39] EU law grants the individual the right not to be subjected to automated decision-making, including profiling.[40]

However, the anti-discrimination relevance of the provision is doubtful for many authors.[41]

First of all, it is pointed out that Article 22 does not even mention the term discrimination and, based on the legislative history of the provision, this absence is read as a deliberate choice to exclude or at least marginalize the anti-discrimination aspect.

During the preparatory work on the GDPR, the European Parliament had proposed to include a reference to non-discrimination in the text of Article 20 (the provision in which the regulation on profiling and automated decisions was originally included).

The text proposed by the European Parliament stipulated: "Profiling that has the effect of **discriminating** against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible **discrimination**

[38] A similar general rule specifically identifying such processes does not exist in American law: see T.Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data' 47 *Seton Hall Law Review*, 995 (2017), 1015.

[39] This reference to the singularity of the provision in relation to the rest of the Regulation will be taken up and explained more fully in the course of the discussion, in particular in section I, 4.1.

[40] Profiling means "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" (article 4(4)). As we shall discuss, it is debated whether profiling per se can be (or always should be) considered an automated decision, even though it cannot be ignored that almost all automated decisions are based on profiling (in order to be more targeted and effective).

[41] See D. Baldini, 'Article 22 GDPR and prohibition of discrimination. An outdated provision?' *CiberLaws*, August 20, 2019, available at *https://www.cyberlaws.it/en/2019/article-22-gdpr-and-prohibition-of-discrimination-an-outdated-provision/* (last access 28 March 2023).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9"." (emphasis added).

Also the European Data Protection Supervisor (EDPS) had suggested in his proposal to include an explicit reference to discrimination: "Measures based on profiling that have the effect of **discriminating** against individuals, on the basis of the special categories of personal data referred to in Article 9, shall be prohibited. The controller shall prevent any possible **discrimination** resulting from such measures"[42] (emphasis added).

Both proposals were then shelved and it was preferred to adopt the version brought forward by the Council, which, with some modifications, substantially corresponds to the one subsequently approved, and which did not contain any references to discriminatory risk or the principle of non-discrimination. [43]

Relying on this legislative history, it has been argued in some quarters that Article 22 has relatively little to do with the inherent issue of discrimination and that this absence should be read as a choice to exclude or at least diminish the anti-discrimination dimension contained in the discipline.[44]

However, notwithstanding legitimate opinions to the contrary, the decision to prefer the text of Article 22 proposed by the Council does not appear to have been motivated by a desire to marginalize the anti-discriminatory relevance therein. This can be inferred first of all from the strong reference to the principle of non-discrimination contained in Recital 71, where there is an explicit mention of the need to avoid discrimination in automated decisions, including profiling.

Recital 71, second paragraph, states that "in order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal

[42] See 'Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations', Amendment 98, European Data Protection Supervisor, 13 (2015), 121, available at *https://edps.europa.eu/sites/default/files/publication/15-07-27_gdpr_recommendations_annex_en.pdf* (last access 3 Apriel 2023).

[43] The Counsil proposal stated: "Decisions referred to in paragraph 1a shall not be based solely on the special categories of personal data referred to in Article 9(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place".

[44] See E. Pehrsson, 'The Meaning of the GDPR Article 22' (Stanford-Vienna European Union Law, Working Paper No 31, 2018), 1-37, 29.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

data are processed, 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 that prevents, 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 that result in measures having such an effect".

Although the recitals, and Recital 71 is certainly no exception, do not have an autonomous operative effect,[45] they are very important both at the systematic level, in that they contribute to framing the legislative act in question within the broader legislative and institutional system of the European Union, and at the interpretative level, in that they play a central role in the interpretation of the binding provisions of an act of the European Union, being able to contribute even in a decisive manner to defining the intent of the operative provision to which they are directly linked (in this case Article 22).[46]

Therefore, it should not be surprising if the Court of Justice has on several occasions relied on recitals to resolve ambiguities of vocabulary, terminology, but also of meaning, context[47] or even to determine the scope of application (more or less broad) of an operative provision.[48]

Recital 71, moreover, as will be discussed more fully in the following paragraphs, does not limit itself to statements of principle but also proposes a number of concrete cases, such as "the automatic refusal of an online credit application or e-recruiting practices without any human intervention", where the risk of discrimination is particularly high.

[45] Case C-308/97, Giuseppe Manfredi v. Regione Puglia, 1998 E.C.R. 1-7685, paraghraps 29-30.

[46] On the central role of recitals in interpreting EU law see: T. Klimas and J. Vaiciukaite, 'The Law of Recitals in European Community Legislation' 15 *Journal of International & Comparative Law*, 61-39 (2008); R. Baratta, 'Complexity of EU law in the domestic implementing process' (19th Quality of legislation seminar "*EU legislative drafting: Views from those applying EU law in the Member States*": European Commission service juridique – quality of legislation team, Brussels, 2014), available at https://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf (last access 21 March 2023).

[47] Among the others, see: Case C-244/95, P. MoskofAE v. Ethnikos Organismos Kapnou, 1997 E.C.R. 1-06441.

[48] Emblematic in this sense: Case C-288/97, Consorzio fra i Caseifici dell'Altopiano di Asiago v. Regione Veneto, 1999 E.C.R. 1-02575.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

As recognized by the same legal literature that downplays the weight assumed by the principle of non-discrimination in GDPR's rules dedicated to automated processing, if interpreted and applied strictly, Recital 71 "has the potential to constitute a substantial burden on companies, which would have to assess the unintended consequences of certain types of automated decision-making".[49]

Conversely, based on the premise that a recital in any case "has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording",[50] it could be argued that it would not have had the same value (but would have had a greater one) if the mention of the discriminatory risk contained in profiling and automated decisions had been included in the binding part of the text of the Regulation.

However, if we put aside the hypothetical register and consider the elements collected in concrete terms, we can rule out the possibility that the mention of the principle of non-discrimination would have represented an additional safeguard with respect to the choice that was then made to provide for a qualified prohibition of decisions based on particularly sensitive data, by referring to Article 9. Indeed, the current text of Article 22(4) excludes the possibility of taking automated decisions based on sensitive data, such as racial and ethnic data, political opinions, religious beliefs, health, sexual orientation and genetic data, subject to exceptions and always provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of the data subject.

One might contend that in the European Parliament's and the European Data Protection Supervisor's versions of the article there was an absolute ban on profiling or decisions based on the profiling of sensitive data. Nevertheless, it is consistent with the Regulation's objective of reconciling the protection of the data subject over his or her own data with the economic needs of the market and businesses to allow for decisions based also on sensitive data (which in itself does

[49] Cfr. E. Pehrsson, 'The Meaning of the GDPR Article 22' (Stanford-Vienna European Union Law, Working Paper No 31, 2018), 1-37, 29.

[50] Case C-162/97, Criminal Proceedings against Nilsson, Hagelgren & Arrborn, 1998 E.C.R. 1-07477 par. 54; Case C-136/04, Deutsches Milch-Kontor, judgment of 24 November 2005 (ECLI:EU:C:2005:716), para 32. This is a common statement in the ECJ rulings, see recently C-418/18 P - Puppinck and Others v Commission

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

not amount to discrimination) while providing a series of safeguards to protect the rights and freedoms of the individual. Moreover, on the one hand it would have been very difficult to identify a discriminatory effect *a priori*, for the reasons already stated on the hardship of abstractly identifying discriminatory algorithmic decisions, [51] on the other hand nothing would have ruled out the possibility of equally or even more discriminatory decisions being made using non-sensitive data, as in the example already seen of "dog owners".

The scope of application of Article 22, in fact, goes beyond the specific subject of discrimination in its legal sense, i.e. discrimination based on grounds protected by special legal provisions (so-called risk factors, such as religion, sex, ethnicity, etc.), as it also extends to those differences in treatment based on apparently harmless grounds, insofar as they are capable of guiding the automatic decision in the direction of unequal and non-transparent treatment of the data subject's rights. Article 22 protects not only the rights and freedoms of data subjects, but also their "legitimate interests", with an intentionally broad and wide-ranging formula in which it is also possible to include those differences in conditions resulting from automated processing of personal data that are inconsistent with or contrary to the requirements of the Regulation.

Evidence along these lines is also to be found analytically in Recital 71(2), where emphasis is placed upon the fact that the right not to be subjected to an automatic decision protects first and foremost the individual's interest in receiving fair, correct and transparent treatment: an interest that an automatic means, without human intermediation, is presumed not to be able to guarantee.

Moreover, the instruction contained therein - and addressed to the data controller - to put in place appropriate technical and organizational measures to prevent discriminatory effects seems to be understood as not being limited to protection against those automatic decisions targeting protected grounds but extending to all decisions based on aspects of the personality of the data subject that are not

[51] Indeed, it is controversial, but we will discuss this later, whether or not references to sensitive data should be included in the instruction datasets of machine learning algorithms in order to prevent direct discriminatory decisions. Designers usually exclude them (precisely to prevent direct discrimination), but this has not prevented their appearance. An attempt was therefore made, by including them together with correctives, to bring about a change in the trend, and the results are comforting.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

relevant to the good or service that is the target of the decision, as suggested literally by the phrase "inter alia" placed between "prevent' and "discriminatory effects". In other words, all those effects, whether or not based on one of the factors protected by the anti-discrimination legislation, that imply a penalization of the person based on aspects of his or her personality without any reasonable consistency with the content of the request or petition must be avoided: aspects that, to the extent that they are taken into account in an automated processing in a decisive manner - i.e. whose consideration has caused a change in the outcome of the decision - give rise to an irregular and therefore unlawful decision. [52]

As a result, in the algorithmic era, in addition to proper discrimination, i.e. perpetrated against protected groups, we have new forms of unlawful automatic processing which, although not covered by any specific rules, give rise to conduct prohibited under Article 22 GDPR, insofar as they unreasonably, unjustifiably and "invisibly" exclude from the enjoyment of goods and services entire categories of individuals.[53]

Patterns have effects that are progressively (but inevitably) destined to expand to other sectors, precisely because they are based on the ability of the computer systems concerned with communicating with each other, exchanging information and replicating past templates, so as to multiply the distorting effects in an uncontrollable manner. In a transversal and unconscious manner, large and varied segments of the population would be deprived of access to goods and services, without any objective economic-legal reason connected to them, other than the reactivity of certain factors possessed by them to trigger the algorithmic response. The non-inclusion in the final text of Article 22 of the reference to discrimination from this point of view proves to be valuable, proving to be a far-sighted choice in order not to harness the response of the European law to ethical and legal structures inspired by the analogical way of interpreting the world, while we faced rapidly

[52] The rationality that must guide us, and to which we must refer exclusively is human rationality, although the algorithm may also have detected in the profile of "dog owners" or "frequent Facebook users" a statistically superior propensity to risk, or lack of punctuality in payments or efficiency in the workplace, for example.

[53] These new types of groups, generated by algorithmic inferences, also face new challenges in terms of organization and collective action. Members of these unusual groups are often unaware that they belong to them. They are therefore less able than historically protected groups to protect themselves from new forms of discrimination.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

evolving phenomena whose developments are still (*rectius* only now) being critically assessed.

The paper is divided into three parts. In the first part, the complex structure of the provision in its various articulations is examined in detail to see what leeway can be afforded to non-statutory discrimination. The second part deals with the rights that Article 22 and Recital 71 confer on the data subject to whom an unlawful automated decision is addressed and the obligations of the controller or processor. While the third and final part deals with the remedies and sanctions that may be invoked by the person subjected to discrimination, whether based on grounds protected by law or not.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

GDPR Feasibility and Algorithmic Non-Statutory Discrimination

Summary: I. The Complex Structure of Article 22. - 1. The Ambiguous Nature of Article 22(1): Prohibition or Right? - 2. The Notion of Automated Decision. - 3. The Uncertain Meaning of an Automated Decision Affecting the Data Subject in a *Similarly Significantly* Way. - 4. Profiling and Associated Decision-Making. - 4.1. Profiling, Individual Decisions and Collective Discrimination. - 5. The problem of *Partially* Automated Decisions. - 6. The Exceptions to the Use of Automated Decision Making. - 6.1. The Contractual Exception. - 6.2. The Law of the European Union or a Member State. - 6.3. The Explicit Consent. - 7. Algorithmic decisions based on sensitive data. - II. Data Subject's Rights and Data Controller's Obligations. - 1. *Ex Ante* Explanation and General Information on the Algorithm's Functionality. - 2. *Ex Post* Explanations, Significant Information and Right to Access. - 3. Right to Access and Effective Exercise of the Right to Contest. - 4. Controller's Obligations and Disaggregated Data. - III. Remedies and Sanctions. - 1. Data Controller's Refusal to Provide Significant Information. Legal Instruments of Coercion in the GDPR. - 2. Breach of Information Obligations and Unfair Damage. - 3. Data Protection Impact Assessment and Damage Imputation Criteria - 4. Compensation for Material and Non-Material Damages Arising from Automatic Discriminatory Decisions.

I. *The Complex Structure of Article 22*

Contrary to appearances, Article 22 is far from being an easily interpretable provision. In fact, it branches out into a number of complicated interpretative problems for which there is no easy answer,[1] but from the settlement on which the verification of whether the provision can constitute an instrument for preventing and combating discrimination and unjustified differences in treatment depends.

[1] See E. Palmerini, 'Algoritmi e decisioni automatizzate. Tutele esistenti e linee evolutive della regolazione', in L. Efrén Ríos Vega, L. Scaffardi and I. Spigno eds, *I diritti fondamentali nell'era della digital mass surveillance* (Napoli: Edizioni Scientifiche Italiane, 2019), 209-244; G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 7.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

The provision, like others in the Regulation, is conceived according to a model in which in the opening paragraph there is the statement of maximum precaution[2] within which the characteristics that must exist in order to make the provision stand are described analytically. This is followed by a list of cases in which automated decision-making is permitted if certain conditions are met, thus constituting an exception to the prohibition. The rights and freedoms to be guaranteed to the data subject and the protective measures to be implemented to guarantee them are then recalled.

Finally, a closing provision is established according to which, even when the conditions allowing the use of automated decisions are fulfilled, it is prohibited to base such decisions on the special categories of sensitive data referred to in Article 9(1), unless further and more restrictive exceptions are invoked and provided that appropriate measures are in place to protect the rights, freedoms and legitimate interests of the data subject.

1. *The Ambiguous Nature of Article 22(1): Prohibition or Right?*

The first problem consists in establishing the nature of Article 22(1), which states "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". Due to its language ("a right not to"), Article 22(1) has been interpreted in two ways: as a general prohibition of processing or as a right to object to automated decision-making.

The prevailing interpretation – also adopted by the Guidelines on Automated Individual Decision-Making and Profiling[3] of Article 29 Working Party (WP29)[4] – is that this is a general prohibition and,

[2] Whether Article 22(1) it is a right of objection or a general prohibition is a question on which the moment of reaction of the legal system depends, and the necessity or lack of a will to react on the part of the data subject, but not the precautionary nature of the measure.

[3] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 19

[4] Article 29 Working Party is an independent European advisory body on data protection and privacy. It is called Article 29 because it was set up under Article 29 of Directive 95/46/EC. It is composed by representatives from the Member States' data

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

therefore, that controllers may not take an automatic decision unless one of the conditions set out in Article 22(2)(a-c) is met first.[5] On the contrary, other scholars argue that the processing is per se lawful and allowed, but the data subject has the right to object to the algorithmic decision: such right prevails over that of the data controller unless one of the exceptions in Article 22(2) applies.[6]

It is important to deepen this debate because the two reconstructions of the preceptive content of Article 22(1) "have a very different impact on the normative strategy for the protection of the human being".[7] The prohibition is, as such, an objective measure, the effectiveness of which is per se and

protection authorities, the European Data Protection Supervisor and the European Commission. The GDPR has replaced it with the European Data Protection Board.

[5] For the majority view, see e.g. M. Brkan, 'Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond', Working Paper 22 February 2018, available at *https://techpolicyinstitute.org/wp-content/uploads/2018/02/Brkan_do-algorithms-rule.pdf* (last access 23 March 2023), the final version is available in 27 *International Journal of Law and Information Technology*, 2, 91-121 (2019); O. Lynskey, 'General Report Topic 2: The New EU Data Protection Regime', in J. Rijpma ed, *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection – XXIX FIDE Congress in The Hague: 2020 Congress Publications* (The Hague: Eleven Publishing, 2020), II, 23-48; P. Perlingieri, 'Sul trattamento algoritmico dei dati' *Tecnologie e diritto*, 1, 181-195 (2020), 184; G. Sartor and F. Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (European Parliamentary Research Service PE 641.530-June 2020), 59; C. Sarra, 'Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of Contestability by Design' 20 *Global Jurist*, 3 (2020). For a critical view see I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 9; O. Sesso Sarti, 'Profilazione e trattamento dei dati', in L. Califano and C. Colapietro eds, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (Napoli: Editoriale Scientifica, 2017) 573-619, 606: F. Lagioia, G. Sartor and A. Simoncini, 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390, 380.

[6] For the minority view, see E. Pehrsson, 'The Meaning of the GDPR Article 22' (Stanford-Vienna European Union Law, Working Paper No 31, 2018), 1-37, 17; L. Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation' 11 *International Data Privacy Law*, 2, 145-162 (2021); L. Bygrave, 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 530-532 (2020).

[7] See R. Messinetti, 'La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata' *Contratto e impresa*, 3, 861-894 (2019), 890, note 89.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

constantly in operation, not requiring any other condition (the protection of the individual works - so to speak - by default). Whereas the functional model of the subjective power of objection requires both the individual's awareness of the existence of an automated decision-making process and the willingness of the individual to object to it.[8] Therefore, it is not surprising that the WP29 preferred the prohibition thesis, because it is more consistent with the systematic purpose of the Regulation to guarantee the individual a measure of control over the determination and circulation of his or her personal identity, as well as with the rationale of the rule in question to safeguard the essence of the individual's power of self-determination in the face of the decision-making power of the technological system.

The wording of the rule, however, seems to support the proposal to interpret the provision as a right of objection. Article 22(1) literally speaks of a right granted to the data subject and does not mention any prohibition. In addition, the placement of Article 22 in Chapter III, which is dedicated to the "rights of the data subject," also seems to be pushing in this direction.

Actually, neither the term 'right' nor the location of the provision can be entrusted with the resolution of the question of whether or not it is necessary for the person concerned to take action to enforce the restraint, since there are rights whose enforcement does not require any effort on the part of the data subject, and in Chapter III itself we find many other provisions in which are laid down rights that take effect without the need to be actively exercised. Although this Chapter concerns the rights of the data subject, the provisions of Articles 12-22 do not exclusively concern the active exercise of rights. As the WP29 guidelines themselves state, not all the prescriptions contained therein refer to situations in which the data subject takes an action, i.e. makes a request, complaint or demand of some kind. Articles 15-18 and 20-21 actually concern the active exercise of a right by the data subject, but Articles 13 and 14 concern duties to be fulfilled by the data controller, without any active involvement on behalf of the data subject. Therefore, the inclusion of Article 22 in Chapter III is not in itself significant with respect to the question whether it is a right of objection or a general prohibition.[9]

[8] See S. Wachter, B. Mittelstadt e L. Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017).

[9] There is some point in underlining that this ambiguity has existed also under the

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Systematically, then, scholars against the line of prohibition argue that other provisions of the GDPR seem to regard purely automated decision-making as generally permitted, beyond and apart from cases where the conditions of Article 22(2) are met. In particular, Articles 13(2)(f), 14(2)(g) and 15(1)(h) provide that data subjects must be informed of the existence of an automated decision-making concerning them, including profiling, as referred to in Article 22(1). This information obligation, according to these authors, "would likely be absurd if automated decision-making would not be allowed under Article 22(1), as it could be read as entailing an obligation to inform data subjects about an activity that would be prohibited under the GDPR".[10]

previous regulation on the protection of individuals with regard to the processing of personal data contained in Directive 95/46CE. The wording of Article 15 of the Directive stated: "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work , creditworthiness, reliability, conduct, etc. . .". The two provisions are very similar and the variations are just a consequence of the different legal tools in which the two provisions are issued (the first is a Directive, while the second is a Regulation). When Article 15 was in force scholars also debated if the disposition had to be interpreted as a prohibition or a right to object: see M. Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', in J. Bus et al eds, *Digital Enlightenment Yearbook* (IOS Press, 2012), 41-56, 50; L. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', 17 *Computer Law & Security Review*, 1, 17-24 (2001); Bird & Bird, 'Profiling and Automated Decision-Taking', available at https://www.twobirds.com/-/media/pdfs/gdpr-pdfs/35--guide-to-the-gdpr--profiling-and-automated-decisiontaking.pdf (last access 22 March 2023). But it does not seem to be a coincidence that, despite the ambiguity, most Member States have decided to transpose the disposition as a general prohibition (Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden, Ireland): see D. Korff, 'New Challenges to Data Protection Study - Country Report: Germany' (European Commission DG Justice, Freedom and Security 2010) 84, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638959 (last access 22 March 2023). Although, other States have adopted a hybrid approach, creating a prohibition for some types of decision and a right to object to other types: for example, Italy, see Article 14 of the Personal Data Protection Code of 2003 (Decreto legislativo 30 June 2003, n. 196). Or in the UK, where the data subject, through written notice to any data controller, is entitled to require that no solely algorithmic decision be taken against him. However, if no such notice has effect and the decision is taken, the data controller must notify the individual that the decision was taken and the individual is entitled, within twenty-one days of receiving that notification, through written notice to require the data controller to reconsider the decision or to take a new decision: see Data Protection Act 1998, s 12.

[10] See L. Tosoni, 'The right to object to automated individual decisions: resolving the

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

However, this argument does not seem convincing.

The two sets of rules have different scopes of application. Articles 13 and 14 impose information requirements for any automated processing of personal data, even if not solely automated and even if not resulting in legal or otherwise significant effects, also with a view to making data subjects aware of the processing in order to allow the timely exercise of rights (e.g. the right to object under Article 21). [11] As has recently been amply argued in the margin of a judgment (oriented in this sense) of the Italian Court of Cassation, the expression "and, at least in those cases", contained in those provisions does not only refer to the cases referred to in Article 22(1) and (4) (i.e. those solely automated), but to 'automated decision-making' in general. [12] Therefore, the expressions 'meaningful information about the logic involved' 'as well as the significance and envisaged consequences of such processing for the data subject' (which already semantically have a much broader scope than Article 22(1), as they also include purely factual consequences) take on a general meaning. [13]

ambiguity of Article 22(1) of the General Data Protection Regulation' 11 *International Data Privacy Law*, 2, 145-162 (2021), 156.

[11] Since automated decisions may be made not only where there is the explicit consent of the data subject, but also where it is necessary for a contract or authorized by Union or Member State law to which the data controller is subject, there could be a situation where an automated decision is made without the data subject having been informed of the existence of an automated decision process concerning him or her beforehand: with the paradox that, in the absence of the notification requirements, data subjects would only become aware of it once the decision has reached him/her.

[12] The Supreme Court (Cass. Civ., Sec. I, 24 March 2021 - 25 March 2021, ord, no. 14381), and the Italian Data Protection Authority ('Provvedimento di blocco del trattamento dei dati personali contenuti in una biobanca n. 389' (6 October 2016), whose legitimacy the Supreme Court was called upon to assess) have implicitly read the provision to mean that the phrase "including profiling, referred to in Article 22(1) and (4) and, at least in those cases" is merely an exemplification of the duty to inform and therefore takes on a general scope for the purposes of Articles 13 and 14. In my opinion, this is not an exemplification but, on the one hand, an effort of clarification in order to avoid that some kind of processing, in particular profiling, could (or would) be overlooked because of its often only preliminary and indicative character; on the other hand, this is an effort to enhance the guarantees, where Article 22(4) on decisions (and profiling) based on sensitive data is mentioned.

[13] See G. Comandé, 'Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali' *Danno e Responsabilità*, 2, 33-42 (2022). A different interpretation, the author convincingly argues, of Articles 13 and 14 would make the rules an imperfect and inadequate duplication of Article 22(1). "If, in fact, a processing leading to automated decision-making were to find its legitimating

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

There is therefore a radical difference between the case of Article 22, which presupposes "a decision based solely on automated decision-making" and which "produces legal effects on the individual or significantly affects him", and that of Articles 13 and 14, which refer generally to any kind of "automated decision-making". The duty to inform, in the latter context, serves to make the data subject aware of the fact that the processing of his or her data triggers an automated decision-making, the importance and consequences of which he or she must be made aware, also because (but this is only a possibility, where no human being is involved) exclusively automated decisions may result from it. [14] The prohibition in Article 22(1), in fact, concerns neither the profiling of an individual per se, nor the performance of an automated (or even exclusively automated) data processing activity, but only the adoption of decisions (wholly automated: to be covered by the prohibition, they must be so characterized) that produce legal effects or, in any event, have significant effects on a person's status. [15]

There are two different scopes of application because the regulatory object of the two sets of provisions is different: that of Articles 13 and 14 is "automated decision-making'", that of Article 22(1) is "automated decisions". Automated decision-making do not always lead to a fully automated decision; on the contrary, it is often a human being who then makes the decision or intervenes significantly in the process to

basis in consent, it would be information about the importance and consequences for the data subject that would make the manifestation of will appropriately 'specific, informed' (Recital 32) 'and of the extent to which this occurs' (Recital 42). Otherwise, if the information were to be provided only when the case of processing completely overlaps with that of Article 22, it would be incomprehensible why it should be included - and repeated - in Articles 13 and 14 rather than directly among the specific guarantees of Article 22 itself, and thus together with the 'right to obtain human intervention by the controller, to express one's opinion and to contest the decision'."

[14] The lack of human control, as pointed out at the outset, could lead to irrational, nonsensical, unfounded, discriminatory or more generically distorted decisions being brought into the economic-legal system, which a human control would probably have realized and avoided (but we will return to this point later in the text, when we discuss the exclusively automated nature of the decision).

[15] See F. Lagioia, G. Sartor and A. Simoncini, 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390, 380. Article 21(1) makes it clear that profiling is per se permissible, and that the data subject has the right to object to it on grounds relating to his or her particular situation when it is based on the grounds set out in Article 6(1) (e) (performance of a task carried out in the public interest or in the exercise of official authority) or (f) (legitimate interests).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

steer it in the way he or she considers most appropriate. Even profiling, which tends to take the form of fully automated processing, is often only a preliminary activity of classifying persons on the basis of their interests; the decision is then taken by a human being, so as to remain outside the scope of the rule (except in cases where profiling already has legal or relevant effects in itself and can therefore be considered as a decision and subject to the Article 22 regime, as we shall discuss).

Scholars interpreting the first paragraph of Article 22 as a right to object and not as a general prohibition of processing argue (and it could not be otherwise under that perspective) that if the decision is based on the explicit consent of the data subject given under Article 22(2)(c), he or she has implicitly waived his or her right to object. [16] The right to contest the decision under Article 22(3) would, still remain at their disposal. The two rights would be enforceable under different conditions and would therefore not constitute unnecessary duplication. The right to object under Article 22(1) would lead to the removal of the automated decision simply by activating the remedy, without the need to present any justification for its exercise other than the fully automated nature of the decision and its significant effects on the data subject. Conversely, the right to contest the automated decision under 22(3) would be a weaker right, since the data subject would not be able to prevent the decision from producing effects simply by expressing his objection: the decision would continue to produce its effects unless human review find any defect or inaccuracy in the decision that would warrant its removal. [17]

While it is true that the exercise of the right to contest does not necessarily imply an *ex novo* decision, with this approach the right to contest under Article 22(3) acquires excessive justifications (and limitations) that are not supported by the text. The right to contest may also be aimed at retracing the basis of the decision, at verifying the reasonableness of the result, beyond (and irrespective of) possible flaws, errors or discrimination (in which case elimination and replacement

[16] See L. Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation' 11 *International Data Privacy Law*, 2, 145-162 (2021), 155; see S. Wachter, B. Mittelstadt e L. Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017), 95.

[17] See L. Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation' 11 *International Data Privacy Law*, 2, 145-162 (2021), 155.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

by another would be an obligation) and beyond and irrespective of human control itself.[18] This perspective, in fact, establishes an inextricable link between the right to obtain human intervention and the right to contest an unsupported decision. In reality, the two rights are independent of each other; it is not necessary to first activate one in order to then have recourse to the other. Without taking into account (though it appears to be a decisive aspect), that nothing excludes the possibility of entrusting this right of contestation, at least at an early stage, to an algorithm equal but opposite to the one that made the decision, designed to detect precisely its mechanisms ("unravelling" the chain of operations into which it is articulated):[19] after all, there is a strong and reasoned inclination to believe that probably only another algorithm is really capable of detecting how another algorithm worked and establishing what another algorithm actually took into account in reaching the decision. [20]

Besides, if we consider Article 22(1) a right of objection, the Data Protection Authorities (DPA) cannot exercise its powers of warning or impose a temporary or definitive restriction on processing, including prohibition (Article 58)(2), if the processing violates the provisions of the Regulation. This would leave the reaction to the controller's wrongdoing to the data subject, who, despite possibly demanding

[18] See A.F. Fondrieschi, 'A Fragile Right: The Value of Civil Law Categories and New Forms of Protection in Algorithmic Data Processing under the GDPR' *Osservatorio del diritto civile e commerciale*, 2, 435-469 (2019), 463, who stated "the real core of the protection against automated decision-making lies (…) in the re-contextualisation of the statistical results of data processing. This aim can be achieved by participating and actively intervening in the decision-making process, that is, by exercising the rights to contest, to express one's opinion, to require human intervention provided for under article 22".

[19] See, for a different opinion that seems to absolutely exclude the possibility of entrusting the right to contest to an automated system, E. Falletti, 'Discriminazione algoritmica' (Torino: Giappichelli, 2022), 174.

[20] See K. Astromskė, E. Peičius e P. Astromskis, 'Ethical and legal challenges of informed consent applying artificial intelligence in medical diagnostic consultations' 36 *AI & Society*, 2021, 509-520, 516; V. Doshi-Velez et al., *Accountability of AI under the law: The role of explanation* (Berkman Center Research Publication Forthcoming: Harvard Public Law Working Paper, 2017); A. Spina, 'New regulation or new medicine: the complex governance of personal data in medicine' 4 *Eur. Data Prot. L. Rev.*, 3, 2018, 280-283; T. Hoeren and M. Niehoff, 'Artificial intelligence in medical diagnoses and the right to explanation' 4 *Eur. Data Prot. L. Rev.*, 3, 2018, 308-319; European Commission High-Level Expert Group on Artificial Intelligence (2019) Ethics guidelines for trustworthy AI, in *https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai*.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

the ongoing unlawful conduct to stop (Articles 18, 79 and 84) and possibly compensation (Article 82), clearly does not enjoy the same means and powers as the supervisory authorities. This does not seem to be consistent with the spirit of the law and the broad powers GDPR grants to DPAs. By contrast, reading the provision as a prohibition, national DPAs could make use of their strong investigative powers (Article 58(1)) to prevent the data controller from using automated decisions if the system of safeguards is lacking or if the data subject's rights and guarantees are not ensured.

In short, ambiguities at the textual level must be resolved on a broader, systematic and teleological plane, by interpreting the provision in the manner most appropriate to its objectives, as a general ex ante prohibition rather than a right of objection. Although the introduction of the consent exception has reduced the importance of the discussion as to whether it is a right or a prohibition (§ 4.2.), the "prohibition line" is the best solution to protect the rights of the data subject, since the controller is prohibited from taking an automated decision regardless of the data subject's willingness (and awareness) to object.[21]

2. *The Notion of Automated Decision*

Automated decisions may originate from private individuals, such as an employer who decides to hire its employees by means of software called upon to select the best profile from among the many CVs sent or, more generally, from commercial entities or organizations, such as banks or financial companies, which decide to recognize or deny a credit line by means of a selection operated by an artificial intelligence program. Examples of this can also be found in Recital 71, which expressly mentions the automatic rejection of an online credit application and electronic recruitment practices without human intervention as examples of automated decisions to which the data subject should not be subjected.

In everyday language, the term "decision" is commonly used to express an evaluation or judgment about a person, fact or thing. Although there may be decisions that have no effect, decisions are

[21] This also avoids that legal protections depend on whether the decision is favorable or unfavorable to the data suject (because if it is favorable, he is unlikely to exercise the remedy).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

usually acts of evaluation that have consequences of some significance.[22] This makes it possible to distinguish decisions from other evaluation processes such as plans, suggestions, advice, mapping of options, which, although they too can be based on a person's evaluation processes and usually produce effects as well, have less incisive, non-binding and not very lasting effects compared to decisions, because they presuppose an evaluation that is not yet (fully) completed.

The reference to the final nature of the decision also makes it possible to distinguish it from internal procedures, which may be intermediate, interlocutory or preliminary, because it normally represents the ultimate synthesis of an evaluation process or, for example, a specific choice between a set of variables.[23] The decision, in essence, is intended to generate effects that are outward-looking, because they are expected to change the external world.[24]

But an automated decision can also be made by a public authority, such as a court ruling or an act of awarding a financial contribution by the public administration.[25] The question arises in this respect whether the silence of Article 22 and, in particular, Recital 71 (insofar as it contains examples of automatic decisions taken only by private parties), corresponds to an intention to exclude decisions taken by public authorities from the scope of the rule.

Article 22 does not distinguish between decisions taken by public authorities or private parties, nor does it give precise indications on the reconstruction of the scope of application of the rule on the basis of the nature of the subject from which the decision originates. But it is precisely this vagueness (in addition to the close link with Recital 71 where, beyond the examples adopted, there are ample references to

[22] After all, if a decision has no effect, it is merely a purpose, a plan, but not a real decision.

[23] See L. Bygrave, 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 530-532 (2020), 532.

[24] This is not withstanding that a conclusive effect cannot result from a decision that is not itself labeled "final": see R. Binns and M. Veale, 'Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR' 00 *International Data Privacy Law*, 0, 1-14 (2021), 11.

[25] See D. Schartum, 'From facts to decision data: about the factual basis of automated individual decisions", *Scandinavian Studies in Law*, 379-400 (2018); M. Suksi, "Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective' 29 *Artificial Intelligence Law*, 87-110 (2021).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

the public dimension of the phenomenon) that leads one to consider the provenance of the decision by a public authority or a private party irrelevant for the purposes of applying the prohibition.

At the same time, because Article 22 does not require any *prima facie* formal requirement, also a process labeled as a plan, letter of intent, advise or "an interim or individual step taken during the automated processing",[26] may fall within the scope of Article 22 if it meets the other legal requirements.[27] As the WP29 emphasised, one should not be guided by labels and, rather, analytically evaluate each individual automatic measure to determine whether or not it falls within the threshold of the rule. However, the materiality threshold is quite high, as will be discussed in more detail in the next section, and indeed seems to have been raised in comparison with the previous regime under Article 15 of Directive 95/46/EC (DPD). This means that this control must be carried out consistently with the intended function of the prohibition, the scope of which is limited to decisions that reach a certain threshold of importance.

3. *The Uncertain Meaning of an Automated Decision Affecting the Data Subject in a* Similarly Significantly *Way*

Article 22 does not cover every type of automatic decision, as they have to produce "legal effects or similarly significantly affecting the data subject". The prevailing approach among scholars under the former Article 15 DPD [28] identified legal effects as those decisions capable of "affecting their legal status"[29] or, in more prosaic terms, those decisions which "impact legal position or legal interests of data subjects".[30]

[26] See D. Kamarinou, C. Millard and J. Singh, 'Machine Learning with Personal Data' (Queen Mary School of Law Legal Studies Research Paper No. 247, 2016), 12.

[27] See L. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', 17 *Computer Law & Security Review*, 1, 17-24 (2001), 19, which expressed its opinion by referring to the former Article 15 of the Data Protection Directive, but did not change its position with the introduction of the new regulation.

[28] The formulation of Article 22 does not differ from its predecessor in this respect.

[29] See M. Martini, 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling', in B. Paal and D. Pauly eds, *Datenschutz-Grundverordnung* (Beck-online, 1nd ed., 2017), 249-265.

[30] See M. Brkan, 'Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond', Working Paper 22 February 2018, available at

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

It is important to highlight at the outset, also in order to distinguish decisions that produce legal effects from those that significantly affect the data subject, that decisions producing legal effects are such insofar as they influence rights already acquired by or accruing to the data subject. Rights that may be based on a law or on a contract.

This reference to the law and the contract has also recently been taken up by the WP29 in its guidelines, which seems to distinguish between effects arising directly from the law and effects arising from the contract binding force. In this sense, the guidelines give two types of examples of rights: those resulting from the law, such as "vote in an election, or take legal action; entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit; refused admission to a country or denial of citizenship"; and those arising under the contract, such as "cancellation of a contract".[31]

More ambiguous (and controversial) is to determine the notion of a decision that "affects the person concerned in a similar significant way". The GDPR does not define the expression, but Recital 71 provides some examples in this regard. The Recital cites the denial of "online credit applications" and "e-recruiting practices" as two examples of automated decisions with significant consequences.

Although these examples help to better outline the scope of the provision, many ambiguities remain regarding the notion of "similarly significant". For example, are effects only significant if we can consider them as such objectively (i.e., independently of the perceptions of the people involved) or also subjectively? Also, do these effects have to be only material or can they be only moral? And again, do the effects have to be negative or can they also be favorable to the data subject?

The doctrine that has dealt with these questions in the context of Article 15 DPD has responded positively to all these questions, stating that the way in which the person concerned perceives the effects of the decision must also be taken into account; that purely non-material damage is also covered;[32] and that the decision may also be favorable

https://techpolicyinstitute.org/wp-content/uploads/2018/02/Brkan_do-algorithms-rule.pdf (last access 23 March 2023), 10.

[31] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 21. This list is not exhaustive and should be seen simply as a typification of some possible decisions affecting the data subject rights.

[32] For a point of view according to which the effects can be both material and /or immaterial, potentially affecting the data subject's dignity, integrity or reputation, see D.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

to the data subject.[33] However, the validity of these opinions must be verified in the light of the new wording of the rule, due to the addition of the adverb "similarly"[34], which was not present in Article 15 DPD.[35]

Despite the introduction of the term "similarly" may also suggest a broadening of the scope of the rule (if understood in the sense of "however"),[36] this addition seems to be intended to make it clear that only those decisions leading to effects of a certain importance will be covered by Article 22. The legislative history shows that the introduction of the adverb "similarly" was a deliberate choice by the lawmaker to reduce the scope of the provision, which was probably considered too broad under the previous version.[37] In particular, through the insertion of this term the legislator wished to establish a stronger bond between decisions producing legal effects and decisions producing significant effects.

In this regard, the question becomes, though, in what terms this connection has to be so close, i.e. what aspect of legal decisions must also be proper to non-legal decisions in order to fall within the scope of the rule. The expression could first of all be interpreted as meaning that decisions should, like legal decisions, have a certain binding force.

Kamarinou, C. Millard and J. Singh, 'Machine Learning with Personal Data' (Queen Mary School of Law Legal Studies Research Paper No. 247, 2016), 12.

[33] See L. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', 17 *Computer Law & Security Review*, 1, 17-24 (2001), 19.

[34] See I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 12; L. Bygrave, 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 530-532 (2020), 534.

[35] Article 15 (1) stated "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

[36] This might be argued if one understood the word "similarly" as excluding any relevance to the fact that the decision produces effects protected by law, in the sense that the decision is relevant "in any event" irrespective of whether or not it has any legal effect, as long as it significantly affects the person. But the background of the rule and the lawmaker's intention can lead to the exclusion of this interpretation.

[37] For the legislative history from which this intention is derived see E. Pehrsson, 'The Meaning of the GDPR Article 22' (Stanford-Vienna European Union Law, Working Paper No 31, 2018), 1-37, 13.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

If we ponder over it, the main effect of a legal decision is its binding force, as the examples of decisions mentioned by the WP29 in its guidelines also show.

However, the meaning with which the adverb was introduced does not seem to be of a technical legal nature, but alludes to the content scope of a legal decision. Rather, it is more consistent to refer the adverb to the general tendency of legal decisions to assume a certain importance for the individual: to vote or not to vote in elections, to receive or not to receive a benefit, to annul or not to annul a contract, are usually decisions that have a significant impact on a person's life. Assuming that it could not already be inferred by interpretation from the wording of Article 15 DPD, the European legislature seems to have wanted to introduce this "new" reference taking as a generalization (although it is known that this is not always the case) that legal decisions possess a particular importance and requiring the "same" importance for the non-legal decision to fall within the threshold.

This reading is also consistent with the interpretation of Article 22(1) as a prohibition and not as a right of objection, since faced with such far-reaching restrictions on the data controller's faculties, it is reasonable that the European legislator should have specularly demanded a high relevance of the decisions affected by the prohibition, again with a view to reconciling respect for the rights of the data subject with the needs of market innovation, in an attempt not to lose ground to foreign markets.

However, it has been argued that if the interpretation I am proposing were to be followed, a number of potentially discriminatory decisions would remain outside the scope of Article 22, such as being permanently banned from a popular social network. [38] But this does not appear to be at all the inevitable outcome of the interpretation we are proposing, as an assessment and distinction will have to be made on a case-by-case basis, depending on the decision under scrutiny and the interests involved. If the decision to ban a user from a social network was for that user productive of significant consequences in terms of injury to his dignity, as well as to his rights to self-expression and to the development of his personality, then it will be considered

[38] See G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 18.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

relevant, as it will have affected the person as much as a legal decision (moreover, the cancelation or not of a contract of little value or easily replaceable may be a far less important decision than being banned from a social network in today's world). [39] Regardless of any financial damage, which might not even be there and the provision would still apply, as we have pointed out.

However, if the expressed view on the significance the decision must have is followed, unlike under the regime of Directive 95/46/EC, subjective perception can no longer be considered sufficient to deem a decision significant, since in order to assess whether the effects have reached the threshold of significance one must consider (1) the decision, (2) the purpose of the decision, and (3) the context of reference in an objective manner, although the concrete analysis of the case could lead to taking into account also the particularities of the individual situation, the proof of which could be facilitated by the use of presumptions. [40]

With regard to the effects, whether they should be negative or can also be positive, the situation is more complex because in some cases, in view of a promotion or advantage, the person may have been subjected to a test or examination that caused him/her harm, not only moral but also economic, or the loss of a further (and more lucrative) opportunity, and for this reason the legislator has raised the protections, which now apply even if the request to enter into the contract comes from the person concerned and has been granted (but this is a topic to which we will return in § 4.1).

This stringent approach is also confirmed by the WP29 guidelines.

According to WP29, from the introduction of the word "similarly" it follows that "the threshold of significance must be similar to that of a decision producing a legal effect". In this regard, the guidelines have clarified that in order for data processing to significantly affect someone, the effects must be sufficiently great or important to be worthy of attention. In other words, the decision must have the

[39] See J. York, 'Getting banned from Facebook can have unexpected and professionally devastating consequences', (Quartz, 31 March 2016), available at https://qz.com/651001/getting-banned-from-facebook-can-have-unexpected-and-professionally-devastating-consequences/ (last access 3 April 2023).

[40] Some scholars express doubts as to whether the significant consequences, especially after the insertion of the adverb "solely", can be entirely emotional: see I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 12.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

potential to significantly influence the circumstances, behavior or choices of the data subjects; have a lasting or permanent impact on him or her; or, in its most extreme form, lead to the exclusion or discrimination of individuals. Despite the obvious difficulty of being precise about what could be considered sufficiently significant to meet the threshold, the WP29 also provides some examples of decisions that could have significant effects: (a) decisions that affect someone's financial situation, such as their creditworthiness; (b) decisions affecting someone's access to health services; (c) decisions that deny someone a job opportunity or put them at a serious disadvantage; (d) decisions that affect someone's access to education, for example admission to university.[41]

These examples, however, are limitedly explanatory, referring to situations in which it is by no means excluded that they are legal positions in the full sense of the term. If we refer to the sphere of human health, the right to receive education – including university education – or the right to work, we are talking about rights recognized by the fundamental principles of EU law as they concern the free development of the personality, and therefore automated decisions that limit them will be decisions that have "legal effects". [42]

It is more difficult to frame decisions concerning someone's financial situation, but in this regard, we have to consider that the correct assessment of creditworthiness is the prerequisite for obtaining a credit reference, i.e. the reputation that the client has with banks and financial intermediaries. The reference, which reflects the correctness of the client's behavior in the context of financing relationships, is important because intermediaries take it into account when deciding whether to grant financing. Being considered a "bad payer" can have negative effects on access to credit, on private initiative, and on one's social and professional relationships. The sensitive area and the effects that the circulation of this information has on consumers' access to credit, have moreover led national legislators to establish specific regulations.[43]

[41] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 22.

[42] See D. Schönberger, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' 27 *International Journal of Law and Information Technology*, 2, 171-203 (2019), 191; C. Sarra, 'Il diritto di contestazione delle decisioni automatizzate nel GDPR' XII *Anuario Facultad de Derecho - Universidad de Alcalá*, 2019, 33-69, 46.

[43] In Italy, for example, there is a code of conduct underwritten by the trade associations

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

4. *Profiling and The Need for Associated Algorithmic Decisions*

Profiling is a form of automated processing which consists in collecting information about an individual (or a group of individuals) in order to assess their characteristics or develop behavioral patterns in order to place them in a certain category or group, in particular to analyze and/or make predictions about them. As the term "included" after "processing" in Article 22(1) suggests, profiling is one of the possible ways of processing on which an automated decision can be based,[44] although indeed it represents the most common forms of processing because it allows for a decision that is more in harmony with the characteristics of the person for whom it is intended to be made. But this does not mean that profiling cannot be used per se – irrespective of the intention to make a decision – or that all algorithmic decisions involve profiling.[45] The W929 guidelines give the example of a speeding fine taken on the basis of camera evidence as an automated decision that is made without profiling first. If, on the other hand, the fine were taken as a result of an assessment involving other factors, such as the subject's driving behavior or other traffic violations, it would instead be profiling.[46]

of industry operators, which is legally binding – if it is not complied with, data processing is unlawful and can lead to sanctions and compensation for damages – and establishes guarantees for those concerned: see Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti [9141941], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9141941 (last access 23 March 2023).

[44] See O. Sassi, 'Profilazione e trattamento dei dati personali', in L. Califano and C. Colapietro eds, *Innovazione tecnologica e valore della persona* (Napoli: Editoriale Scientifica, 2017), 573-628, 606; M. Iaselli, 'Sanzioni e responsabilità in ambito GDPR' (Milano: Giuffrè, 2019), 49; A. Pierucci, 'Elaborazione dei dati e profilazione delle persone', in V. Cuffaro, R. D'Orazio and V. Ricciuto, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 413-451, 421.

[45] See E. Pellecchia, 'Privacy, decisioni automatizzate e algoritmi', in E. Tosi ed, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (Milano: Giuffré, 2019), 417-439, 427; A. Caia, 'Sub Article 22', in G.M. Riccio, G. Sforza and E. Bellisario eds, *GDPR e Normativa Privacy Commentario* (Milano: Wolters Kluwer, 2018), I, 219-229, 223; A. De Franceschi, 'Sub Article 4', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 153-176, 161.

[46] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 8. They argue that the inclusion of the expression

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

However, the prohibition (as well as the regime of exceptions and safeguards) of solely automated decisions applies to profiling when it is followed with algorithmic decision that produces legal effects or is likely to significantly influence the data subject.[47] In the legal framework for automated decision-making, profiling is in fact normally relevant to the extent that it is accompanied by an algorithmic decision.[48] The requirement that profiling be connected by a decision in order to fall within the scope of application can be inferred from the wording of Article 22 and Recital 71, as well as from the legislative history of the provisions.

Tracing the evolution of Article 22, both the elimination of any reference to 'personal aspects' (which now appears only in Recital 71) and the elimination of the criterion of 'intention' which appeared in the text of Article 15 DPD (and which is now completely absent from the text of the Regulation, including Recital 71) are important.[49] The latter results in a reduction of the possibility that profiling falls within the scope of the prohibition when it remains at the level of automated processing preparatory to the final decision (from which the necessary legal or significant effects derive).[50] It also excludes situations of mere attempts to profile that do not achieve the decision stage.

Moreover, the failure to reproduce the ambiguous verb "assess" also seems to be part of the design of the legislature to exempt profiling from the scope of the rule. Aside from the example that is frequently mentioned of a clothing retailer using profiling to classify customers according to what they might like, even when profiling is used by companies and government

"including profiling" as an aside between two commas is significant of the fact that for the lawmaker profiling is not a mandatory step but only a possible (albeit very common) step in view to take an automated decision.

[47] See G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 17.

[48] In the absence of a decision-making process, profiling alone is still subject to guarantees under Articles 13 to 15 (see Recital 72).

[49] Article 15(1) stated: "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data **intended** to evaluate certain personal aspects relating to him, such as his performance at work , creditworthiness, reliability, conduct, etc". (emphasis added).

[50] For a partially different view see see I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 13.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

agencies to classify and rate people for more important goods or services, it does not mean that it in itself produces "significant" effects just because we are dealing with more important or valuable items. Significant effects arise from the decision to refuse or deny a good or service, not from the classification itself: from profiling to decision-making, for example, a human action could intervene that, considering other factors, grants the benefit despite the contrary outcomes of the classification.

The condition that profiling be followed by a decision in order to be covered under automated-decision rules is also evident when considering the GDPR legislative history. When the draft GDPR was first published, it had been suggested by the Working Party that Article 22 should cover not only the outcome of profiling, but also "profiling as such, i.e. the creation and the use of personal profiles by data controllers, before a measure or even decision is taken which has an effect on the data subject".[51] This option was explicitly discarded by the GDPR lawmaker,[52] reflecting its desire to narrow the scope of Article 22[53] compared to the previous Article 15 DPD in which, conversely, profiling was more broadly prohibited per se under certain conditions.[54]

However, this does not exclude the fact that, in practice, profiling can have "significant" effects once, depending on the circumstances, it is potentially decisive. This may be the case even if no decision is taken on the basis of the profiles detected, or if the decision that is then formally taken is merely reproductive or a mere consequence of the profiling activity carried out previously (and no significant human intervention has taken place).[55] If the classification itself has legal or particularly significant

[51] Article 29 Working Party, "Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation" (13 May 2013), para 2(a). 3

[52] See Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', 17 *Computer Law & Security Review*, 1, 17-24 (2001), 20.

[53] This intention to narrow the scope can also be deduced from the fact that Article 20 of the original wording of the Commission's proposal (available at *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF*) (last access 24 March 2023) was entitled "Measures based on profiling" to underline how the individual was protected by measures (the word "decision" did not even appear) taken against him as they were based on profiles and the actual profile creation.

[54] See A. Savin, 'Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks' (Paper presented at *7th International Conference Computers, Privacy & Data Protection*, Brussels, 2014), 1-15, 3.

[55] See Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

effects, profiling could exceed the threshold of significance and be considered on a par with a decision, aided by the fact that, as mentioned above, Article 22 does not require any formal "labeling". The reference in Recital 71 to "profiling" as a form of automated processing that assesses personal aspects relating to a natural person, such as "personal preferences or interests (…) or behaviour", falls under Article 22 to the extent that profiling becomes so important that it reaches the threshold of decisiveness. This is where it is possible to apply the rules (i.e. the ban) on algorithmic decision-making to profiling as such, the result of which is an improper differentiation in the goods and services offered to costumers.

On this issue, further clarifying developments could result from a case that has been submitted to the Court of Justice and is pending.

On 25 October 2021, the Administrative Court of Wiesbaden decided to refer two preliminary questions to the Court of Justice concerning the scope of protection under Article 22 against automated decision-making and profiling in the context of the calculation of an individual's credit score.[56] At the time of writing, the outcome of the ECJ ruling is not yet known, but the importance and sensitivity of the issue is already evident from the referral and factual background. The case regards a claim filed after an individual was refused a loan on the basis of a low score provided to a bank by SCHUFA.[57]

The person concerned asked SCHUFA to provide access to the information in its disposal and to delete several entries from its

Series No. 2017-20), 1, for whom profiling "*has the potential to curtail the increasingly widespread use by businesses and government agencies of automated methods for categorizing, assessing and discriminating between persons*". See also A. Savin, 'Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks' (Paper presented at *7th International Conference Computers, Privacy & Data Protection*, Brussels, 2014), 1-15, 2, which, in relation to the Directive in force ratione temporis, maintained that "*profiling (gathering of data and forming profiles based on this data) has the potential to be harmful even if no decisions are made on the basis of profiles*."

[56] See Case C-768/21, available at *https://curia.europa.eu/juris/showPdf.jsf;jsessionid=75D380D7634B1FB9C496C9CE6D8DB163?text=&docid=254364&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2320568* (last access 24 March 2023).

[57] Creditworthiness information in Germany is mostly monitored and recorded by SCHUFA Holding AG, Germany's largest credit agency. SCHUFA is the abbreviation for Schutzgemeinschaft für allgemeine Kreditsicherung, meaning "general credit protection agency". SCHUFA provides essential credit information for those wishing to live and operate financially in Germany. The credit score reflects the extent to which a person has fulfilled financial obligations, such as bills and credit card payments, and is used to decide how worthy he or she is of additional obligations, such as personal loans.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

database. While SCHUFA informed the person about his score and provided basic information about how the score calculation worked, it did not divulge details about what data was taken into account and how it was weighted, claiming that that information was protected as business secrets and therefore should not be released. The latter defends itself by claiming that it merely calculates scores to assess people's creditworthiness, that it predicts, on the basis of this score and other characteristics of the person, the likelihood of future behavior (e.g., repayment of a loan), and that it shares this information with its clients (such as banks in this case, but also insurance companies or other economic entities). Credit rating agencies argue that, by calculating the score and sharing it with their clients, they merely profile people and do not make any automated decisions within the meaning of Article 22, as the actual decisions about people are made by their clients, and thus do not have to comply with the transparency requirements and entitlements contained therein.

The person filed a complaint with the supervisory authority of Hesse State (Hessen DPA), which rejected the complaint on the basis that SCHUFA generally complies with Section 31 of the German Federal Data Protection Act (BDSG), which governs the calculation and use of retail scores, and with the case law that preceded the GDPR. The Hessen State Control Authority also found no evidence in this case of a possible breach by SCHUFA of the GDPR requirements, and came to the conclusion that the scoring methodology should not be disclosed. The person, faced with the negative decision, started court proceedings against the Hessian DPA and SCHUFA. This application to rectify the adverse decision taken by the Hessen State Control Authority was dealt with by the administrative judge in Wiesbaden.

The German court examined the case and decided to refer to the CJEU to clarify whether the calculation by credit agencies of an individual's credit score and the disclosure of this score to third parties without further comment or recommendation falls within the scope of the provision. The German judges held that it was possible to argue that even the mere processing of the score constituted a relevant "decision" under Article 22; and noted that even if in theory the customer of the credit agency (a bank, a telecommunication operator or a homeowner) could make a different decision on the basis of indicators other than the score value (citing examples where people with a good score were nevertheless refused a loan), in practice credit scores play a decisive

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

role in the granting of loans and in the elaboration of loan conditions, and insufficient score values lead to the refusal of consumer loans in most cases.[58]

4.1. *Profiling, Individual Decisions and Collective Discrimination*

The European legislator, by loosening the legal link between automated decisions and profiling, seems to have narrowed the guarantees for the data subject - profiling is not subject to the prohibition as it was under the previous DPD system - however, by doing so, the legislator has broadened the scope of Article 22 from the point of view of individual decisions based on collective profiling.

In line with the general *ratione personae* scope of application of the GDPR, [59] the textual interpretation of Article 22 seems to leave collective decisions outside the normative regime of the Regulation, i.e. those decisions that affect groups of people linked by common characteristics, such as living in a certain area, belonging to a certain ethnic community, sharing a certain characteristic, but also being the owner of an animal or being a member of the local gym. The exclusion of automated collective decisions from the scope of the GDPR was assessed as a huge flaw. [60]

However, this strongly negative judgment seems only partially supportable because collective decisions are not entirely excluded from the Article 22 scope, even though it literally refers only to "individual" decisions.[61] In this regard, we have to distinguish between decisions that affect an individual but are based on group profiling and decisions that are based on group profiling and actually affect a whole range of people.

[58] For more details and further references see J. Finlayson-Brown – G. Catharina, 'German Court asks CJEU to clarify whether calculating consumer credit scores falls within the scope of automated decision-making under GDPR', available at *https://www.allenovery.com/en-gb/global/blogs/digital-hub/german-court-asks-cjeu-to-clarify-whether-calculating-consumer-credit-scores-falls-within-the-scope-of-automated-decision-making-under-gdpr* (last access 23 March 2023).

[59] GDPR only covers the protection of natural persons (Article 1(1)) and hence governs only the protection of individuals and not groups.

[60] See M. Brkan, 'Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond', Working Paper 22 February 2018, available at *https://techpolicyinstitute.org/wp-content/uploads/2018/02/Brkan_do-algorithms-rule.pdf* (last access 23 March 2023), 8.

[61] Article 22 is entitled "automated *individual* decision-making".

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

As examples of the first type, we can recall the case of behavioral scoring (or, more specifically, creditworthiness by associations) reported by the Financial Times, according to which a successful black American businessman had received a letter from his credit card operator informing him that his credit limit had been reduced from $10,800.00 to $3,800.00.[62] In this case, the reduction of the credit card limit was not based on the customer's personal credit history but on the fact that he had shopped in outlets popular with people with a bad credit history.[63]

As an example of the second type of scenario, i.e. collective decisions affecting a whole range of individuals, we can consider imposing a higher insurance premium on individuals associated with a particular zip code.[64] Another example is the one that seems to have been conducted by Amazon with respect to people based on their residency, which led to the exclusion of particular US Zip codes from access to the Amazon Prime same-day delivery service. According to an analysis by Bloomberg these postal codes represent predominantly black neighborhoods.[65]

Under the previous regime of Article 15 DPD, the decision to which a person could contest had to be based on his or her profile, since it had to be directed at assessing "certain personal aspects relatinng to him or her". This link between the personality profile and the measure taken, which had moreover been strengthened by the Commission's initial reform proposal, has been abandoned by the GDPR. In the GDPR the decision may be based on any form of automated processing, including personality profile or collective profile, as long as it produces legal effects or affects a data subject in a similarly significant way.[66] In this regard,

[62] See M. Hurley and J. Adebayo, 'Credit Scoring in The Era of Big Data' 18 *Yale Journal of Law & Technology*, 148-216 (2016), 150.

[63] See T. Alloway, 'BIG data: Credit where credit's due' *Financial Times* (February 4, 2015), available at https://www.ft.com/content/7933792e-a2e6-11e4-9c06-00144feab7de (last access 24 March 2023).

[64] See E. Pellecchia, 'Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation' *Nuove leggi civili commentate*, 5, 1209-1235 (2018), 1227.

[65] See D. Ingold and S. Soper, 'Amazon Doesn't Consider the Race of Its Customers. Should It?' (April 21, 2016), available at https://www.bloomberg.com/graphics/2016-amazon-same-day/ (last access 24 March 2023). However, Amazon has categorically denied that race was a factor in deciding which postcode areas would be covered by the service and instead argued that its primary consideration was the cost associated with providing same-day delivery.

[66] The use of the word "included" before "profiling", all enclosed in commas, reinforce the separation between profiling and automated decision, thus making the decision a result independent of profiling.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

the WP29 guidelines consider the possibility that "similarly significant effects could also be triggered by the actions of individuals other than the one to which the automated decision relates" and they excluded that the collective nature of profiling does rule out the applicability of Article 22 protections.[67] Therefore, collective profiling is covered by the GDPR (to the extent that it is used for individual decision-making).

In this respect, however, it has been argued that if decisions are based on anonymous data (as is often the case when profiling is collective) then the regime would not apply because, according to Recital 26 GDPR, the "principles of data protection should … not apply to anonymous information".[68] Nevertheless, it should be made clear, on the one hand, that anonymization of personal data is not sufficient to exclude the application of GDPR if the data subject still remains identifiable[69] and, on the other hand, that even if the decision is based on the processing of anonymous data, [70] protection against

[67] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 22.

[68] See L. Edwards and M. Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' 16 *IEEE Security & Privacy*, 3, 46–54 (2018), 49; F.J. Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' 24 *The International Journal of Human Rights*, 10, 1572-1593 (2020).

[69] In addition, with the increasing importance and use of big data, the re-identification of an individual belonging to a certain group is greatly facilitated: see C. Perlingieri, 'Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi' *Actualidad Jurídica Iberoamericana*, 12 bis, 836-847 (2020), 841.

[70] This also applies to models, which do not refer to identifiable persons. A predictive model that says "80 per cent of the people living in postcode XY0 pay their bills late" does not refer to natural persons. Since the model is not personal data, the Data Protection Regulation does not apply. However, when such a predictive model is applied to a person, things change. When a company applies the model to a person, the information becomes relevant because it relates to that person due to its purpose or result. The effect is that the company, by directing, for example, an advertisement to a person although identified on the basis of nameless data (the company might have a list of websites visited and a list of interests deduced for the person with a cookie with ID xyz on his or her computer), treats that person differently from others; it identifies him or her through a result. The information may therefore also refer to a person because of its purpose, if a company uses the data "relates to, (i.e. is about) a person's characteristics or behaviour to influence that particular person": see Article 29Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136), 20 June 2007-, 9. Delves eminently into the subject F.J. Zuiderveen Borgesius: see 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation' 32 *Computer law & Security Review* 256–271 (2016), 260; 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' 24 *The International Journal of Human Rights*, 10, 1572-1593 (2020), 1581.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

automated decisions may equally apply if it has the effect of *singling out* a person.[71]

As WP29 noted, automated decisions can be based on any type of data.[72] If it is likely that Article 22 was designed on the assumption that the decision "will ultimately involve the processing of data of that person as the right it lays down is operationalized by reference to the data subject",[73] this does not mean that the decision cannot be based on the processing of another person's data or even non-personal data (at least not in a final stage).[74] Hence also the reference made in the Introduction to the atypical and peculiar character of Article 22, as if it represents in some ways an independent island from (and within) the rest of the Regulation's prescriptions.

Bringing collective profiling under the automatic decision regime does not mean that Article 22 is readily applicable with respect to

[71] See Article 29Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136), 20 June 2007, 12-13.

See for an opposite approach D. Kamarinou, C. Millard and J. Singh, 'Machine Learning with Personal Data' (Queen Mary School of Law Legal Studies Research Paper No. 247, 2016), 10; G. Resta, 'Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza' *Politica del diritto*, 2, 199-236 (2019), 223; P. Zuddas, 'Intelligenza artificiale e discriminazioni' *Consulta Online*, 16 March 2020, available at *https://giurcost.org/LIBERAMICORUM/zuddas_scrittiCostanzo.pdf* (last access 28 March 2023), 1-18, 16.

[72] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 8.

[73] See L. Bygrave, 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 530-532 (2020), 533, who however considers that if the decision is based on profiling it must be based on personal data, arguing from the definition of profiling in Article 4 (4).

[74] This conclusion was even more evident under the original wording of the Commission's proposal in 2012, in which the final text of Article 22 referred to a "natural person" and not to a "data subject": see A. Savin, 'Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks' (Paper presented at *7th International Conference Computers, Privacy & Data Protection*, Brussels, 2014), 1-15, 9, according to which *"the fact that Regulation would apply to natural person means that profiling is covered in the Regulation, in principle at least, irrespective of whether the data is anonymized or not"*. However, the substitution with the word "data subject" does not seem to preclude the advanced interpretation, since Article 22 does not impose as a further requirement that the data on which the decision is based must relate to the person to whom it is addressed, nor that they must be identifiable data. The focus of the article seems only to be on the decision, the means used to adopt it, and the effects it has on a particular individual, not on the nature of the data used to process and take it.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

collective discrimination. In this regard, there may arise the problem that, unlike the consumer category, "data subjects [are] not aware of the identity of other members of the group/have no relationship with them and have limited perception of their collective issues".[75] However, this problem is mitigated by the recognition of the possibility for collective bodies to intervene under Article 80 to protect general interests against violations of the GDPR, even in the absence of an individual mandate. A view that can be supported now more than ever in light of the European Court of Justice's ruling handed down in the case *German Federation of Consumer Organisations (and Associations) (Verbraucherzentrale Bundesverband) v. the Irish branch of Facebook (now Meta Platforms)*.[76]

5. *The Problem of* Partially *Automated Decisions*

In order to apply Article 22(1) prohibition the decision must be based *solely* on automated processing[77]. The provision in this respect has not changed compared to Article 15 DPD.

According to the literal meaning of the term "solely" scholars have argued that even minimal human intervention would prevent the decision from being considered fully automated and thus preclude application of the provision.[78] This strict reading of the term "solely"

[75] See A. Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection' 32 *Computer Law & Security Review*, 2, 238-255 (2016). On the implications between artificial intelligence and consumers discrimination see S. Lanni, 'Dataquake: intelligenza artificiale e discriminazione del consumatore' *Nuovo diritto civile*, 2, 97-123 (2020).

[76] Court of Justice of the European Union, 28 April 2022, C-319/201, Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e V., available at *https://curia.europa.eu/juris/document/document.jsf?text=&docid=258485&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=205442* (last access 6 April 2023).

[77] On the other hand, however, if the decision is based on profiling, it is not necessary that it also be carried out exclusively by automated means; in fact, the decision is considered to be based exclusively on automated tools even when a human being plays a substantial role in the creation of the relevant profile.

[78] See 'EU Citizens might get a 'right to explanation' about the decisions algorithms make', available at *https://cyberlaw.stanford.edu/press/eu-citizens-might-get-%E2%80%98right-explanation%E2%80%99-about-decisions-algorithms-make* (last access 24 March 2023). Original publication: 'EU Introduces 'Right to Explanation' on Algorithms' *Fusion*, July 5, 2016. See also M. Hildebrandt, 'The Dawn of a Critical Transparency Right for the

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

was reflected in a German case, also involving the rating agency SCHUFA.[79] In this case, the court was called upon to decide whether the credit-scoring system could fall within the scope of the German rules transposing Article 15 DPD,[80] even though the automated system concerned only the preliminary investigation phase (collection and verification of the documentation relating to the subject to be assessed). The answer was negative precisely because it was supported by the argument that a human being, regardless of his or her powers, had in any case intervened after that phase and before the (at least) formally decisional phase.[81]

This interpretation is also consistent with the intention of the lawmaker. We can discover this intent from the rejection of the amendments proposed by the European Parliament to the European Commission's draft aimed at adding the word "predominantly" to the measures to which Article 22 would apply.[82]

However, it is likely that this lawmaker's aim will find opposition from the ECJ, which has already expressed arguments in favor of a less restrictive view of what "human control" entails.[83] This

Profiling Era', in J. Bus et al. eds, *Digital Enlightenment Yearbook* (IOS Press, 2012), 41, 50, that in reference to the European Commission's 2012 draft, explains why human intervention will render Article 20 inapplicable. See Wachter, B. Mittelstadt e L. Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017), 92: "*the phrase 'solely' suggests even some nominal human involvement may be sufficient*". See M. Martini, M. Martini, 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling', in B. Paal and D. Pauly eds, *Datenschutz-Grundverordnung* (Beck-online, 1st ed., 2017), 249-265.

[79] This is a different and earlier case than the one cited above that gave rise to the ECJ preliminary ruling. The SCHUFA credit rating agency has given rise to several court judgments over the years.

[80] The case pre-dated the entry into force of the Regulation, which, however, as noted, made no changes on this point.

[81] See Judgment of the German Federal Court : BGH: Umfang einer von der SCHUFA zu erteilenden Auskunft BGH, Urteil vom 28 January 2014 – VI ZR 156/13 (LG Gießen, AG Gießen) 490.

[82] See European Parliament Committee on Civil Liberties, Justice and Home Affairs, "Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) COM(2012)0011 – C70025/2012 – 2012/0011(COD)", available at *https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_EN.html* (last access 24 March 2023). It is clear that the Parliament wanted this amendment to widen the scope of the application of the provision.

[83] See CJEU Opinion 1/15 of the Court (Grand Chamber) on the EU-Canada Passenger Name Record (PNR) Agreement, 26 July 2017, available at *https://eur-lex.europa.eu/legal-*

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

approach in fact inevitably results in a reduction of the data subject's protection, because a long list of potentially significant decisions would remain outside the scope of the Regulation. To stay with the example of credit scoring,[84] the algorithm gives a rate (that represents the result of the analysis of potential customers) and the companies usually just apply specific conditions or deny services depending on the algorithmic rating. Normally, this "human" decision does not require any evaluation effort from the controllers, so much so that the "truly" "human" nature of this "decision" has even been question.[85] If we follow the approach that any human intervention classifies the decision as not fully automated, companies could bypass Article 22 by

content/EN/TXT/PDF/?uri=CELEX:62015CV0001(01)&from=EN (last access 13 June 2022). According to the Court, *"since the automated analyses of PNR data necessarily involve some margin of error, as stated in paragraph 169 of this Opinion, any positive result obtained following the automated processing of that data must, under Article 15 of the envisaged agreement* [stipulating that 'Canada shall not take any decisions significantly adversely affecting a passenger solely on the basis of automated processing of PNR data'], *be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the air passengers concerned is adopted. Consequently, such a measure may not, under Article 15, be based solely and decisively on the result of automated processing of PNR data"*.

[84] This is one of the riskiest sectors in terms of indirect discrimination or, in US language, in terms of disparate impact, in our data-driven society: see J. Knutson, 'Credit Scoring in the Insurance Industry: Discrimination or Good Business?' 15 *Loyola Consumer Law Review*, 4, 315-329 (2003), 318; B. Reddix-Smalls, 'Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market' 12 *UC Davis Business Law Journal*, 1, 87-124 (2011); F. Ferretti, 'The Legal Framework of Consumer Credit Bureaus and Credit Scoring in the European Union: Pitfalls and Challenges-Overindebtedness, Responsible Lending, Market Integration, and Fundamental Rights' 46 *Suffolk University Law Review*, 3, 791-828 (2013); T. Zarsky, 'Understanding discrimination in the scored society' 89 *Washington Law Review*, 1375 (2014); F. Pasquale, 'The Black Box Society: The Secret Algorithms That Control Money and Information' (Cambridge-London: Harvard University Press, 2015), 98 and 196; S. Barocas and A. Selbst, 'Big Data's Disparate Impact' 104 *California Law Review*, 3, 671-732 (2016), 684; G. Biferali, 'Big data e valutazione del merito creditizio per l'accesso al peer to peer lending' 34 *Diritto dell'informazione e dell'informatica*, 3, 487-509 (2018); K. Langenbucher, 'Responsible A.I.-based Credit Scoring – A Legal Framework' 31 *European Business Law Review*, 4, 527-572 (2020); L. Ammannati and G.L. Greco, 'Il credit scoring alla prova dell'intelligenza artificiale', in U. Ruffolo ed, *Intelligenza artificiale. Il diritto, i diritti, l'etica* (Milano: Giuffrè, 2020), 373-386; P. Manes, 'Credit scoring assicurativo, machine learning e profilo di rischio: nuove prospettive' *Contratto e impresa*, 469-489 (2021); J. Lerman, 'Big data and its exclusions', 66 *Stanford Law Review Online*, 55 (2013).

[85] See G. Malgieri – G. Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' 7 *International Data Privacy Law*, 4, 243-265 (2017), 251.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

simply ensuring an even nominal human intervention at the automated process end. [86]

These outcomes were considered unacceptable in terms of data subject fundamental rights protection by other scholars, who have proposed a relative notion of "solely", based both on the *ratio legis* of the GDPR and on a different interpretation of the wording of Article 22(1).[87]

As far as the Regulation's intent, only a less strict view would be able to cover the full scope of Article 22 as described at Recital 71, in which automatic refusals of an online credit application and e-recruiting practices are mentioned, as examples of decisions from which the data subject shall be protected. According to this broader approach, decisions "formally attributed to humans" , but originating "from an automated data-processing operation the result of which is not actively assessed by either that person or other persons before being formalized as a decision", would be included in the scope of automated decision-making discipline. [88] The consequence is that Article 22(1) still applies "even though a nominal human intervention formally 'takes' the decision but the entire 'preparatory evidence and discretional judgments (e.g., scoring) are fully based on automated means'".[89]

[86] Which is what Ryan Calo provocatively suggests: "*All a firm needs to do is introduce a human—any human, however poorly trained or informed—somewhere in the system,*" and "*[V]oila, the firm is no longer basing their decision 'solely on automated processing*.' See 'EU Citizens might get a 'right to explanation' about the decisions algorithms make', available at *https://cyberlaw.stanford.edu/press/eu-citizens-might-get-%E2%80%98right-explanation%E2%80%99-about-decisions-algorithms-make* (last access 24 March 2023). Original publication: 'EU Introduces 'Right to Explanation' on Algorithms' *Fusion*, July 5, 2016.

[87] Paul Voigt and Axel von dem Bussche, 'Rights of Data Subjects', in P. Voigt and A. von dem Bussche eds, *The EU General Data Protecton Regulaton* (Cham: Springer, 2017), 181

[88] See Article 16(3)(i), DPD Amended Proposal, Brussels 15 October 1992, COM (92) 422 final – SYN 287, 26, available at *https://aei.pitt.edu/10375/1/10375.pdf* (last access 13 June 2022): "what is prohibited is the strict application by the user [data controller] of the results produced by the system. *Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgement must have its place*. It would be contrary to this principle, for example, for an employer to reject an application from a job-seeker on the sole basis of his results in a computerized psychological evaluation, or to use such assessment software to produce lists giving marks and classing job applicants in order of preference on the sole basis of a test of personality" (italics added).

[89] See G. Malgieri – G. Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' 7 *International Data Privacy Law*, 4, 243-265 (2017), 251.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

This enlarged approach seems to have convinced WP29 as well.[90] Actually, the Working Party in its guidelines stated that "solely" means that there should not be any human involvement in the decision processing. However, shortly after that initial statement, the WP29 – almost as if they wanted to clarify their approach – add that "the controller cannot avoid the Article 22 provisions by fabricating human involvement"; such as "if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing". According to the Working Party, to qualify as human involvement, "the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data". Shortly before, they also claimed that "if a human being reviews and takes account of other factors in making the final decision, that decision would not be 'based solely' on automated processing".

Nevertheless, this interpretation did not erase any doubts among scholars. On the contrary, according to some commentators, the WP29 has created more confusion than there was previously, because it has generated the problem of determining how far a human intervention must be extensive (and intensive) in order to be able to consider a decision as not based solely on automated processing.[91]

First of all, in this way the WP29 seems to overestimate what a human being can do in the conclusive phase of a processing entirely based on automatic means. With the concrete risk of having a countervailing effect if we just consider the burden of responsibility on the human being involved in the final stage of the procedure. As has been pointed out, in such cases the human being faces a dilemma: either to confirm the decision taken by the machine, or to change it but to be ready to give his/her organization specific explanations as to why the machine – usually so efficient – should be considered unreliable in the specific case. Since this could be a very difficult task, due to the fact that algorithmic decision-

[90] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 20.

[91] See G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 19.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

making systems can be extremely complex and opaque, the human being involved would be more likely to confirm the decision taken by the machine simply because "it could be extremely difficult for her/him to justify the specific reasons why the decision taken by so an accurate tool needs to be changed".[92] With the effect, for the heterogeneity of ends, that the data subject would be deprived from human control in all those situations where human intervention can represent a barrier against the distortions of the automated processing by providing a contribution of empowerment and greater understanding that the algorithm clearly cannot provide alone.[93]

Secondly, the approach of WP29 seems to deny any value to the human intervention carried out in the stages leading up to the decision. It focuses only on the need for a human intervention in the final processing phase, forgetting that, in complex decision-making systems, the human being can be reserved a substantial role in a previous stage rather the final one, without thereby excluding the automated character of the decision.[94] To this extent, the decision of the Italian Data Protection Authority in a number of recent cases concerning food delivery applications, in which each rider was assigned a score, through specific and predetermined parameters, which allowed him/her to have priority access to the "time slot selection system", is emblematic. According to the Italian Data Protection Authority, even if the parameters on the basis of which the algorithm works are set by a human being, this does not mean that the decisions are not based exclusively on automated processing and that therefore the corresponding rules do not apply.[95]

[92] See C. Sarra, 'Il diritto di contestazione delle decisioni automatizzate nel GDPR' XII *Anuario Facultad de Derecho - Universidad de Alcalá*, 2019, 33-69.

[93] Whether the ECJ adopts the approach that human intervention only counts if the person could have "an actual influence on the result" an issue around the burden of proof will arise. For this event, it was argued that the burden of proof should be placed on the complainant because, otherwise, the "company would face the daunting task of proving after the fact that additional information could have changed the final outcome": see E. Pehrsson, 'The Meaning of the GDPR Article 22' (Stanford-Vienna European Union Law, Working Paper No 31, 2018), 1-37, 11. However, place the burden of proving that no human involvement played role in the final decision on the data subject could turn into "diabolic proof" and deter the recourse of the data subject's right safeguards in Article 22(3).

[94] See C. Kuner, D.J.B Svantesson., F.H. Cate, O. Lynskey and C. Millard, "Machine learning with personal data: is data protection law smart enough to meet the challenge? 7 *International Data Privacy Law*, 1, 1-2 (2017), 2.

[95] Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Despite these ambiguities,[96] what really matters is that even for WP29 it is incontrovertible that "solely" does not mean without any human involvement but without any "significant" human involvement.[97]

6. *The Exceptions to the Use of Automated Decision Making*

The general prohibition set in Article 22(1) has some relevant exceptions.

The controller is entitled to undertake the processing if the decision is: (a) necessary for the performance of or entering into a contract; (b) authorized by Union or Member State law; or (c) based on the data subject's explicit consent.

These exceptions are characterised by such breadth and vagueness that they call into question the view according to which Article 22 GDPR reflects the European legislator's scepticism towards fully automated decision-making processes as harbingers of bias and potentially sources of errors, given the lack of prior control of human beings.[98]

In comparison with the previous regime contained in Article 15 DPD, the introduction of express consent as an additional exception immediately stands out. Apart from that, which is the most important innovation, in general terms these exceptions replicate, increase and to some extent strengthen the exceptions contained in Article 15(2) DPD.

di Foodinho s.r.l. - 10 giugno 2021 [9675440], in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9675440* (last access 24 March 2023); Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 July 2021, in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994* (last access 24 March 2023).

[96] The ambiguities are probably due to the differences within the Working Party members, between those who wanted to remain more faithful to the literal interpretation of Article 22 and others who wanted to expand its semantic field.

[97] That has been the opinion also expressed by the UK Information Commissioner's Office recently, Feedback request – profiling and automated decision-making, 2017, 19, available at *https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf* (last access 24 March 2023).

[98] See M. Brkan, 'Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond', Working Paper 22 February 2018, available at *https://techpolicyinstitute.org/wp-content/uploads/2018/02/Brkan_do-algorithms-rule.pdf* (last access 23 March 2023), 7.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

6.1. *The Contractual Derogation*

An automated decision may be lawfully taken if it is necessary for entering into or performing a contract between the data subject and the controller. The contractual derogation was laid down in Article 15 (2)(a) DPD, but the GDPR legislator has changed its content to a large degree, on the one hand by restricting its scope and on the other hand by extending it.

To begin with, the exception has been limited to the cases when algorithmic decision-making is necessary to enter into a contract or for its performance. The Data Protection Directive, while identifying a connection between the decision and the contract, did not go as far as to indicate an explicit necessity criterion, providing only that the decision must have been made "in the course of the contractual process" (Article 15(2)(a)).[99] The addition of this criterion undoubtedly makes it more difficult for the data controller to escape Article 22(1) by simply entering into a standardized contract with the data subject. [100] However, much will depend on how the courts interpret the necessity criterion, because Article 22 does not define when automated decision-making is "necessary".

The authors who have dealt with this issue have ruled out the possibility that the necessity criterion can be applied so rigorously that it functions as one of indispensability, arguing that it would be difficult to think of an example where an automated decision would necessarily have to be made without human involvement.[101] The WP29 interpreted it restrictively without going so far as to consider it as an indispensability criterion, arguing that controllers may only use automated decision-making for contractual purposes if they believe

[99] Accordig to Article 15(2), Member States shall provide that a person may be subjected to an automated decision if: "*(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view*".

[100] See I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 15.

[101] See L. Bygrave, 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 530-532 (2020), 536.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

it is the most appropriate way to achieve the objective.[102] Routine human involvement may sometimes be impractical or impossible due to the huge amount of data processed.[103] In any case, the controller must be able to demonstrate that such processing is necessary, taking into account that a less privacy-invasive method could be adopted.[104] If there are other effective and less invasive means to achieve the same objective, the processing would not be "necessary". Otherwise the "necessity" criterion would be arbitrarily defined by the controller.

Another important amendment to the previous text was the elimination of the condition in Article 15 DPD that the contractual proposal had to come from the data subject and not from the data controller. In other words, the exception now applies even if the contract was proposed by the controller and the data subject merely adhered to it. This obviously broadens the scope of the derogation, but it is an expansion compensated by an overall higher level of protection for the data subject. However, this broadening of the derogation scope seems to be compensated by an overall higher level of protection for the data subject. In fact, in the previous regime the imposition of "appropriate measures" to safeguard his/her legitimate interests, such as arrangements allowing him/her to share his/her point of view, were not imposed if the person's request to enter into or perform the contract had been fulfilled.

[102] For example, such automated processing seems to be necessary for the conclusion and execution of an insurance contract, in order to accurately estimate the risks of personal injury or traffic accidents and thus decide whether to agree to insure a person or a driver. For further details, see S. Landini, 'Insurtech: innovation in production, distribution, governance, and supervision in the insurance market' *Assicurazioni*, 3, 433-446 (2021); E. Battelli, 'Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi'*Corriere giuridico*, 12, 1517-1526 (2019); G. D'Ippolito, 'Processi decisionali automatizzati nel settore assicurativo. Un'indagine preliminare' *MediaLaws*, available at https://www.medialaws.eu/wp-content/uploads/2019/03/2-2019-dIppolito.pdf, (last access 24 March 2023).

[103] The guidelines give the example of a company that places an advertisement for a job and receives tens of thousands of applications with attached CVs. Because of the exceptionally high volume of applications, the company might find that it is practically impossible to identify suitable candidates without first using complete means of recruitment. In this case, an automated decision-making process may be necessary to draw up a short list of possible candidates. See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 23

[104] See G. Buttarelli, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit European Data Protection Supervisor' (11 April 2017), 8.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

The derogation was duly criticized because it operated on the fallacious assumption that satisfying a person's request to enter into or perform a contract was never problematic for that person.[105]

6.2. *The Law of the European Union or a Member State*

The law of the European Union or of the Member State to which the data controller is subject may authorize the adoption of solely automated decisions. Measures to safeguard the rights, freedoms and legitimate interests of the data subject must be provided (Article 22(2) b). The exception was already contained in Article 15(2)b DPD, but the reference to the rights and freedoms of the data subject has been newly added. This addition seems to be relevant with regard to the question of whether the European Union or the member states should encompass the rights in Article 22(3) or whether they may instead provide for other, different measures. Uncertainty arises because the exception in Article 22(2)b) is not referred to in Article 22(3), which begs the question whether, as regards automatic decisions permitted by EU or Member State law, the rights to obtain human intervention, to express one's opinion and to contest the decision, should be granted. On the other hand, however, the exception in Article 22(2)b), unlike the other two, already includes within it a reference to the need for EU law or national laws to provide for appropriate measures to protect the rights, freedoms and legitimate interests of individuals affected by automated decision-making: as indicating an accomplished system where when it comes to EU or Member State laws, the safeguards are established directly by those entities, without going through those indicated in Article 22(3).[106]

[105] See L. Bygrave, 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', 17 *Computer Law & Security Review*, 1, 17-24 (2001), 21. The latter proposes as an example a situation in which a decision on a person's job application is made on the basis of psychometric tests. Yet this type of test may have detrimental consequences for the person concerned (and for the quality of job application processes in general), even if he/she is granted the job. For example, the person may consider such a test as demeaning to his or her dignity, or the test may not reveal that the person is qualified for a more advanced position.

[106] Different considerations seem to apply to the exceptions to the prohibition of basing automated decisions on sensitive data (Article 22(4)), which, as we shall observe, is not considered to be exempt from the measures of Article 22(3) even when the authorization comes from the laws of the EU or the Member States.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

With regard to the obligation for Member States to enact laws incorporating the guarantees of Article 22(3), the WP29 guidelines are somewhat ambiguous. They state that the laws of "Member States authorizing [algorithmic decision-making] must also incorporate appropriate safeguards". They then add that "such measures should include, at a minimum, a way for the data subject to obtain human intervention, express his or her point of view and views, and challenge the decision".[107] This has led some authors to suggest that the GDPR harmonizes safeguards, even when a Member State creates a new exception to the prohibition of automated decision-making.[108] However, other scholars, analyzing the regulations of single States, have noted that they have already developed variations on Article 22 safeguards. Some States have even extended the safeguards recognized under the GDPR: French law has allowed for algorithmic administrative decisions, which entitles the administration to an explanation;[109] Italian law that has chosen to allow for the exercise of the rights under Articles 15-22 also to persons acting on behalf of the deceased data subject (with some exceptions, including the will of the data subject).[110] On the contrary, other Member States have reduced the guarantees in their national data protection law.[111]

The Member States' autonomy in establishing the concrete and specific safeguards to accompany the authorization of automated decisions should not, however, lead to a reduction of the rights and safeguards provided by the GDPR for the data subject. That is to say, Member States remain free to adopt the measures they deem most appropriate, but only in the sense of the concrete measure adopted, not the substance of that measure (such

[107] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 27.

[108] See M.E. Kaminski, 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189 (2019), 206.

[109] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (Digital Republic Act, law no. 2016-1321) and decree in March 2017 (R311-3-1-2).

[110] Italian law has chosen to allow for the exercise of the rights under Articles 15-22 also to persons exercising an interest of their own as their representative, or for family reasons deserving protection (Article 2-terdecies Italian Data Protection Code, D.lgs. 196/2003, as amended by Article 2, paragraph 1, lett. f), D.lgs. 101/2018, no. 101). This was also possible because recital 27 of the GDPR specifies that the Regulation does not apply to the data of deceased persons, but allows Member States to provide rules on their processing.

[111] See G. Malgieri, 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations' 35 *Computer Law and Security Review*, 1-26 (2019).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

as, for instance, a mandatory right of explanation on the French model for the automated process of administrative decisions entrusted to a human being, rather than the adoption of a conversion algorithm to which such a right might be assigned).[112] A significant indicator in this respect seems to be the already mentioned strengthening of the reference to the rights and freedoms of the data subject.[113]

With regard to the areas in which a Member State might introduce a law permitting automated decisions, Recital 71 states that this could include the control and prevention of fraud and tax evasion, or to ensure the security and reliability of a service provided by the controller. An example of a Member State's law allowing for automated decision-making is the German law implementing the GDPR, which expressly allows for automated decisions in the field of insurance, as well as in the field of administrative acts within the framework of a fully automated administrative procedure.[114] However, national authorities do not have precise limits and can therefore allow algorithmic decisions for a potentially infinite number of purposes.

Recital 73 (see also Article 23) states that national and EU laws may impose restrictions on the rights granted to the data subject in respect

[112] The safeguards of Article 22(3) are not a *numerus clausus*, so States could provide for additional measures in their laws.

[113] For a different opinion see L. Bygrave, 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 530-532 (2020), 537; E. Troisi, 'AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla intellegibilità dell'algoritmo' *European Journal of Privacy Law & Technologies*, 1, 41-59 (2019), 44. According to some scholars, Article 22(2)b) is not subject to the safeguards of Article 22(3) because of the greater guarantee offered by the legal authorization: see F. Laviola, 'Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa' *Biolaw Journal*, 3, 389-440 (2020), 425. In these cases, it is argued, automation is not left entirely to the initiative of the data controller for its own interests, but is assessed by the legislator in a balance with the public interest that will be expressed in the regulatory framework. Now, in that framework the structures for challenging an automated decision already exist, namely those that configure the organization of justice, so providing for their further establishment would have been pleonastic: C. Sarra, 'Il diritto di contestazione delle decisioni automatizzate nel GDPR' (*Anuario de la Facultad de Derecho de la Universidad de Alcalá*, 2019), XII, 33-69, 56.

[114] Automatisierte Entscheidungen im Einzelfall einschließlich Profiling) of the Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

of "decisions based on profiling" to the extent that this is necessary and proportionate to, *inter alia*, safeguard public security, the prosecution of criminal offences or the execution of criminal penalties, breaches of ethics for regulated professions, and other important objectives of public general interest, such as the maintenance of public registers, provided that such restrictions comply with the requirements laid down in the Charter and the European Convention on Human Rights. This wide openness to the possibility of reducing rights, although tempered by compliance with the subject's fundamental principles and rights, has been viewed with suspicion by scholars.[115]

6.3. *The Explicit Consent*

The GDPR also allows for automated decision-making if it is based on the explicit consent of the data subject (Article 22(2)(c). This is an exception that was not contained in Article 15 DPD.

Article 22(2)(c) is a provision that does not provide much indication, except for the "explicit" character that consent must have in order to authorize the adoption of a solely automated decision. This reference to the explicit nature of consent recalls its form, which must be given in writing, for example, or in any event freely and unambiguously, and refers to the particular gravity of the act. In fact, the GDPR resorts to the adjective "explicit" when particular protection risks for personal data are at stake, so a high level of individual control is required (see below the link to Article 22(4).

Unlike the Commission proposal, which expressly subjected consent to automated decisions to the requirements of Article 7, which sets out the conditions for consent for the processing of personal data, Article 22, in its then adopted version, made no reference to it.[116] Therefore, a legitimate doubt might arise that the conditions laid down in Article 7 for consent to the processing of personal data do not apply to consent to automated decisions.

[115] See G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 20.

[116] See Proposal for a Regulation of the European Parliament and of the Council Commission's, Brussels, 25.1.2012, COM(2012) 11 final (available at *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF* 34) (last access 24 March 2023), 55.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

But this does not seem to be the reason why the reference to Article 7 was dropped, rather its unnecessary and redundant nature. Just as the explicit character of consent does not mean that the other characteristics by which consent is defined in general terms are not applicable.[117] It is merely a necessary addition, justified by the particular gravity of the activity for which consent is given.

Article 22(2)(c) does not specify what information (*if any*) should be provided to the data subject. Nevertheless, from the connection with Articles 4(11), 7(4) and Recital 43, we can reconstruct the characteristics that consent must possess in order to constitute a valid exception. It must consist of a free, specific, informed and unambiguous indication of the data subject's wishes, and if it is given in performance of a contract, its necessity in relation to the performance of the contract from which the service originates must be assessed.

The obvious imbalance between the data subject and the controller in assessing whether consent has actually been freely given leads us to consider the (first) pretense behind the use of consent, i.e. that of conditional offers (which create "take it or leave it" situations): scenarios where the data subject is left with no alternative, if he/she wants to access the good or service, but to give consent to be subjected to a decision based solely on automated processing.

According to Article 7(4), "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". Consequently, "take it or leave it" situations should be assessed as not fully allowed, and thus taken in the absence of the conditions that make it legitimate, if it is based on consent given conditionally to the performance of a service, but for reasons not necessary for the performance of the contract on which it depends.[118]

[117] See F. Lagioia, G. Sartor and A. Simoncini, 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390, 283.

[118] See I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 17. For more extensive critiques on consensus see R. Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality', in S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne, S. Nouwt eds, *Reinventing data protection?* (Dordrecht: Springer, 2009), 83-110, 87.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Even when the processing of personal data is really necessary for the realization of the contract or service,[119] consent should not be deemed to have been freely given if the data subject is unable to make a genuinely free choice or is prevented from refusing or withdrawing consent without detriment, as set out in Recital 42 GDPR.[120] Otherways, the explicit consent of the data subject "is not a real choice between possible alternatives and cannot therefore represent either a means of defense or a form of control".[121]

In legal literature, the significant example of an automated system used to check people's state of need with a view to granting benefits has been given;[122] it is clear that in this case consent cannot be considered free (at least in the absence of a valid alternative, e.g., a semi-automated system or an equally efficient and prompt human system). In other cases, the advantage of enjoying a certain good or service may avoid the harm produced by exclusion from a social context, [123] resulting from the impossibility of access to socially widespread services, and therefore often represents an objective for which the person concerned would not hesitate to give consent. [124]

[119] Consider a very large number of applications and the impossibility, if not extremely time-consuming, for a human being to process all that volume of requests.

[120] See the concerns of A. Astone, 'Autodeterminazione nei dati e sistemi A.I.' *Contratto e impresa*, 2, 429-448 (2022), 439.

[121] See S. Rodotà, 'Elaboratori elettronici e controllo sociale' (Bologna: Zanichelli, 1973), 45. See also the statement of the Italian Guarantor for the protection of personal data that considers the freedom of consent assumption of uncertain consistency if the adherence to the treatment is a prerequisite in order to take advantage of the intended product or service: 4 July 2013, no. 330, doc. web. no. 2542348, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348 (last access 13 June 2022). At all events, relying solely on the consent of the person concerned for the use of certain services or the attainment of certain benefits may not be ethically correct, since the person concerned – perhaps in a weakened condition – may feel compelled to consent even against his or her interest or even dignity: see M. Franzoni, 'Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale', in U. Ruffolo ed, *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (Torino: Giappichelli, 2021), 339-355, 344.

[122] See F. Lagioia, G. Sartor and A. Simoncini, 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390, 383.

[123] See G. Biferali, 'Big data e valutazione del merito creditizio per l'accesso al peer to peer lending' 34 *Diritto dell'informazione e dell'informatica*, 3, 487-509 (2018), 490.

[124] The European Court of Justice has held that consent to the storage of information or access to information, by means of cookies installed in the terminal equipment of the user of an Internet site, is not validly given where the consent results from a pre-selected checkbox, and this is irrespective of whether the information in question constitutes personal data. The case concerned an online gaming service: see C-673/17 - Planet49.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

In the light of these situations, the European Commission's original proposal to exclude the derogation of consent "where there is a significant imbalance between the position of the data subject and the controller" takes on a poignant meaning.[125] If this proposal had been followed, the legal basis should have remained exclusively contractual, at least for certain types of contracts characterised by a clear imbalance of power (such as the relationship between insurance or credit institutions and data subjects). The contractual exception, unlike the explicit consent exception, has on its side the criterion of the necessity of the automated decision, which limits its use by the controller. In these terms, when dealing with highly asymmetrical relationships, the controller should have demonstrated that the fully automated process was necessary (in the terms outlined in the previous section) for the conclusion or performance of the contract.

Not to mention that in some cases, in particular with regard to decisions based on profiling, it may be problematic to trace whether the consent obtained online was actually "explicit" or not. Profiling is often carried out without the data subject even being aware of it, and if the data subject has not given explicit consent to profiling, he or she has not consented to a decision taken on such basis.[126] In other cases, profiling is based only on data derived or inferred from other data, and consensus turns out to be a very insufficient instrument to legitimize the automated processing.[127] This is the reason why decisions based on profiling should comply with special guarantees of legitimacy, requiring for example the adoption of techniques of effective prior information on the specific processing methods that have been authorized.[128]

[125] See Proposal for a Regulation of the European Parliament and of the Council Commission's, Brussels, 25.1.2012, COM(2012) 11 final (available at *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF* 34) (last access 24 March 2023), in particular Article 7(4) and 20(2)c).

[126] For example, explicit consent to cookies should not necessarily mean consent to an automated decision based on such profiling. See M. Brkan, 'Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond', Working Paper 22 February 2018, available at *https://techpolicyinstitute.org/wp-content/uploads/2018/02/Brkan_do-algorithms-rule.pdf* (last access 23 March 2023), 12

[127] E. Falletti, 'Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche' 36 *Diritto dell'informazione e dell'informatica*, 2, 169-206 (2020), 173, complains that, in the light of experience, the exception concerning the expression of consent could take the form of a superficial and habitual authorization of automated decision-making service users, through the absent-minded and formal expression of consent on modules displayed, for example, by banners.

[128] See European Data Protection Supervisor, "*Opinion 7/2015. Meeting the*

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Finally, but this is a topic we will deal with later as well (see § II), it is worth asking how explicit consent can be obtained in relation to a process that may be non-transparent.[129] In other words, it may be far-fetched to ask for explicit consent with regard to a decision whose reasoning process will not be known. In this regard, some reflections of the Italian Privacy Supervisor and the Italian Supreme Court may come into consideration in a case concerning a platform that calculated a so-called "reputation rating" to allow third parties to check its credibility, with the aim of fighting the creation of fictitious profiles. The Italian court affirmed that the consent relating to the processing of personal data given at the time of registration on the platform cannot logically also be valid as acceptance of an automated system that uses an algorithm for the objective evaluation of personal data, where the executive scheme in which the algorithm is expressed and the elements considered for this purpose are not made known.[130]

7. *Algorithmic decisions based on sensitive data*

Automated decisions cannot be based on special categories of data identified in Article 9(1). This provides a list of categories of personal

challenges of big data. A call for transparency, user control, data protection by design and accountability", available at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (last access 24 March 2023).

[129] See C. Kuner, D.J.B Svantesson., F.H. Cate, O. Lynskey and C. Millard, "Machine learning with personal data: is data protection law smart enough to meet the challenge? 7 *International Data Privacy Law*, 1, 1-2 (2017), 1; G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 20; D. Kamarinou, C. Millard and J. Singh, 'Machine Learning with Personal Data' (Queen Mary School of Law Legal Studies Research Paper No. 247, 2016), 15.

[130] See Garante per i dati personali, Provvedimento no 488, 24.11.2016, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5796783 (last access 24 March 2023); Corte di Cassazione, 24.3.2021, no 14381, available at www.italgiureweb.it. In another case - concerning a preliminary verification of an automatic processing system of personal data aimed at monitoring users' driving style in order to give them a score - the Italian Garante had already clarified that the data controller's information notice would have to disclose which parameters were used to assess driving style as well as the consequences: for more information see L. Liguori, 'Sub Articles 13-14', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 289-304.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

data considered sensitive: racial and ethnic data, political opinions, religious and philosophical beliefs, trade union membership, health, sex life, sexual orientation and genetic and biometric data.[131]

Again, while the first part of the provision establishes a *prima facie* general prohibition for data controllers, the second part provides for a number of relevant exceptions, so as to severely soften the initial prohibition. There are two possible exceptions to the prohibition, namely the explicit consent of the data subject for one or more specific purposes set out in Article 9(2)(a), and when such automated decisions are necessary for reasons of substantial public interest and have a basis in EU or Member State law under Article 9(2)(g).[132]

Regarding the first exemption, the express consent invoked by Article 9(2)(a), and referred to in Article 22(4), does not differ in its primary structure from the express consent invoked elsewhere in the Regulation and should therefore be interpreted according to the criteria of Article 7 as discussed in the preceding subsection, save for one exception, of no small importance, which will be discussed shortly. An important safeguard, which is not provided with respect to the counterpart exception regarding non-sensitive personal data, is that EU or national laws may decide that the prohibition on processing sensitive data "may not be lifted by the data subject" (Article 9(2)a). This limitation seems particularly relevant, and should be enhanced by Member States, given both the particularly sensitive nature of the data on which this processing is based and the easiness with which the data subject usually gives consent.

As for the second exception, the possibility that such automated decisions are considered by the law of the Member States as necessary for reasons of public interest increases the possibility – already inherent in Article 22(2)(b) – that national regimes will increasingly differ with regard to the exceptions to the ban of Article 22(1). Nevertheless, this does not necessarily represent a weakening of the data subject's protections, because the relevant law, as already required under

[131] It seems worth noting that these categories of data overlap substantially with the so-called "protected grounds" that are part of EU anti-discrimination law, as reflected in Article 21(1) of the European Charter of Fundamental Rights.

[132] For further details see A. Thiene, 'Sub Article 9', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 240-249, 240; M. Dell'Utri, 'Principi generali e condizioni di liceità del trattamento dei dati personali', in V. Cuffaro, R. D'Orazio and V. Ricciuto eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 179-245, 231.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Article 22(2)(b), must ensure that suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. However, it is not specified what these measures should consist of.

A significant pointer in this respect seems to be offered by the placement of Article 22(4) at the end of the provision and by its wording. Article 22(3), when it deals with the rights to be guaranteed to data subjects and the measures to be implemented to safeguard them, does not mention the exception in Article 22(2)(b), reinforcing the impression, as already pointed out, that automated decision-making authorized by EU law or by a Member State's law follows internally closed, self-serving logics. Article 22(4), on the other hand, does not exempt the same exception based on public grounds relevant to the EU or a Member State's law from the requirement of appropriate measures to protect the data subject's rights, freedoms and legitimate interests, and indeed places it on the same footing (and treats it in the same way) as explicit consent. Therefore, it seems logical to assume, given also the sensitivity of the data on which these automated decisions are based, that these measures should at least guarantee the same rights already granted to the data subject by Article 22(3): i.e. human intervention, the right to express one's opinion and to contest the decision.[133]

The biggest problem concerning automated decisions based on sensitive data is that, despite the ban, and the highest possible safeguards that can be demanded, artificial intelligence technologies challenge the application of the prohibition, as they are able to derive sensitive information (such as a person's gender or ethnicity) from information that is not classified as such (the "likes" put on social network accounts, the websites visited, the place of residence or the shopping location, etc.).[134] There may in fact be additional information linked to membership of a protected group. Persons or groups that suffer unequal

[133] See I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 19, which, however, seem to include only the right to request human intervention.

[134] See F. Lagioia, G. Sartor and A. Simoncini, 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390, 385; see N. Turner lee, P. Resnick e G. Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms", 22 May 2019, available at https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ (last access 9 March 2023).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

treatment are often identified by the value of proxy information, such as citizenship, residence, country of birth: information that does not fall into the sensitive, and therefore protected, categories, but which may give rise to discrimination and unfairness.

For this reason, too, it has been suggested that sensitive information should no longer be excluded from the construction process of automated decision-making (as is often the case, as mentioned at the beginning, in order not to incur in blatant direct discrimination). Of course, once the model is ready, sensitive information should not take on weight as a variable for decision-making. From a regulatory point of view, this has an important implication: the collection of sensitive personal data would become necessary to ensure the fairness of the algorithms and the legislator should find reasonable ways to allow their use in the model-building process but without generating the risk of a discriminatory decision. [135]

II. *Data Subject's Rights and Data Controller's Obligations*

The GDPR recognizes a number of safeguards for an individual affected by an automated decision.[136] Article 22(3) requires the

[135] In the UK there has been a movement in favor of collecting data on ethnicity for the very purpose of being able to detect discrimination. Strong arguments have been made for the use of ethnic identifiers in data collection in order to be able to detect discriminatory treatment and outcomes. In fact, including this information could be not only necessary to detect discrimination, but also to correct the algorithm: see I. Chopin, L. Farkas and C. Germaine, 'Ethnic origin and disability data collection in Europe-Comparing discrimination' (*Migration Policy Group for Open Society Foundations*, 2014), available at https://www.opensocietyfoundations.org/uploads/d28c9226-bed7-4b1b-ac8b-4455f3c3451a/ethnic-origin-and-disability-data-collection-europe-20141126.pdf (last access 24 March 2023); I. Zliobaite and B. Clusters, 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models' 24 *Artificial Intelligence and Law*, 2, 183-201 (2016). See also B. Goodman and S. Flaxman, 'European Union regulations on algorithmic decision-making and a "right to explanation"'38 *AI Magazine*, 3, 4 (2017), which point out that including not only variables that are explicitly named, but also any variables with which they are correlated also suffers from a number of complications in practice. With relatively small data sets, it may be possible to identify and account for correlations between sensitive and "non-sensitive" variables. However, as data sets become larger and larger, correlations may become increasingly complex and difficult to detect. With sufficiently large data sets, the task of exhaustively identifying and excluding a priori data characteristics related to "sensitive categories" may be impossible.

[136] For an illustrative overview on data subject's rights see F. Piraino, 'I "diritti

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

controller to put in place appropriate measures to safeguard the data subject freedoms and legitimate interests, demanding that at least the rights to obtain human intervention, to express their points of view and to contest the decision are ensured. These rights seem to be organized in a progressive order of protection: from a minimum given by human intervention to a maximum given by a true juridical-dialectical structure capable of absorbing the others, going much further, thus leaving the data subject the choice of which means to use before requesting full-fledged judicial protection.[137]

Their effectiveness depends first and foremost on the quality, quantity and, above all, relevance of the information and explanations that the data subject can receive from the controller.[138] However, a problem arises in this regard, as far as the right to explanation is not mentioned in Article 22 GDPR or in any other article. The only instance where it is mentioned is Recital 71, which states that processing under Article 22 "should be subject to suitable safeguards, which should include (…) the right to obtain human intervention, to express his or her point of view, *to obtain an explanation* of the decision reached after such assessment and to challenge the decision". (italics added).

On the existence or non-existence of a right to an explanation, a heated debate has arisen among specialists. Some held that this right was not guaranteed, others the opposite. However, the existence of a right to an explanation is no longer controversial per se, but what is in dispute is the content of this right, whether the data subject is only entitled to a general *ex ante* explanation of how the algorithm works, or a right to an *ex post* explanation of the decision concretely and individually made against him or her[139].

dell'interessato" nel regolamento generale sulla protezione dei dati personali', in R. Caterina ed, 'GDPR tra novità e discontinuità', *Giurisprudenza italiana*, Sezione monografica, 2789 (2019); A. Ricci, 'I diritti dell'interessato', in G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna: Zanichelli, 2017), 179-250; F. Di Ciommo, 'Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio', in V. Cuffaro, R. D'Orazio and V. Ricciuto eds, *I dati personali nel diritto europeo* (Torino: Giappichelli), 353-390 (2019), 35; F. Casilai, 'I diritti dell'interessato', *ivi*, 327.

[137] See C. Sarra, 'Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of Contestability by Design' 20 *Global Jurist*, 3 (2020), 8.

[138] See U. Pagallo, 'Algo-Rhythms. The Beat of the Legal Drum' 31 *Philosophy and Technology'*, 4, 507-524 (2018).

[139] This approach of the debate on the existence and content of the right to an

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Once we have addressed these two positions, and the alternative perspectives aimed at overcoming the radicalness of the debate, we will consider the obligations of the data controller towards the data subject's requests, focusing also on the relevance of disaggregated data.

1. Ex Ante *Explanation and General Information on the Algorithm's Functionality*

In view of its non-binding nature, according to some scholars, Recital 71 would not be sufficient to ground the right to explanation,[140] because, as the European Court of Justice has repeatedly pointed out, recitals are not legally compulsory. Therefore, they do not create any rights or obligations contrary to or not inherent in the articles.[141]

Besides, the legislative history would show the intention of the lawmaker to exclude a right to explanation from the mandatory rules and leave it as a good practice whose implementation is left to the free initiative of the controller or to the legislative initiative of the national states (which can always increase the protections for the data subject).[142] The reference to the right of explanation in Recital 71 it would to be framed in this sense: on the one hand, as a warm recommendation addressed to the controller to provide a full understanding of the decision-making processes, also *ex post*; on the other hand, as an incitement to national legislators to enhance the protection of the data subject's rights.[143]

explanation of automated decisions is shared by F. Geburczyk, 'Automated administrative decision-making under the influence of the GDPR-Early reflections and upcoming challenges' 41 *Computer law & Security Review*, 2021, 105538, 6.

[140] See S. Wachter, B. Mittelstadt e L. Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017), 80.

[141] See, e.g., CJEU, Giuseppe Manfredi v. Regione Puglia, Case C-308/97, Judgment of 25 November 1998, paras. 29–30; CJEU, Criminal Proceedings against Nilsson, Hagelgren & Arrborn, Case C-162/97, Judgment of 19 November 1998, para. 54.

[142] On the legislative history that would make clear that lawmakers have deliberately excluded an *ex post* right to explanation of specific decisions see S. Wachter, B. Mittelstadt e L. Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017), 81; E. Pehrsson, 'The Meaning of the GDPR Article 22' (Stanford-Vienna European Union Law, Working Paper No 31, 2018), 1-37, 28.

[143] As France has done, for example, for automated administrative decisions, as illustrated above (see § I, 6.2.).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Also, to the argument (which we will return to in the following section) - advanced by the proponents of the existence of a right to an ex-post explanation - that such a right would be based on the aforementioned Articles 13(2)(f), 14(2)(g) and 15(1)(h), which grant the data subject the right to know from the controller whether there is an automated decision-making, including profiling, and to have meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing, authors opposed to the configurability of such a right to an explanation point out that the right to receive information on the processing is quite different from the right to obtain explanations on the logic followed by the algorithm in making the decision. Rather than a detailed explanation of the system's internal logic after a decision has been taken, Articles 12-15 aim at providing a comprehensive overview of the envisaged processing activities, which enhances the data subject's understanding of the scope and purpose of automated decision-making.[144] In this respect, Article 12(7) clarifies that the purpose of Articles 13-14 is to provide "in an easily visible, intelligible and clearly legible manner a meaningful overview of the *intended* processing" (italics added).[145] The focus of these articles, from the perspective of these authors, seems to be on the near future and the likelihood of a decision being made.

Stance that they maintain even when faced with the possibility of the right to access being exercised after the decision has been made. According to those who argue for the existence only of a right to an ex ante explanation of the algorithm's functionality, the right to access would follow the time constraints of Articles 13(2)(f) and 14(2)(g), and thus data controllers could only limit themselves to sharing information available at the beginning of the process, when the data were collected, not also those processed afterwards.[146]

[144] See S. Schulz, 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall', in P. Gola ed, *Datenschutz-Grundverordnung Vo (EU) 2016/*679 (German: Verlag C. H. Beck, 1nd ed., 2017), 410-419; L. Franck, 'Sub Article 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person', in P. Gola ed, *Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar* (German: Verlag C. H. Beck, 2nd ed., 2018), 390-405; S. Rodway, 'Just How Fair Will Processing Notices Need to Be Under the GDPR' *Privacy & Data Protection*, 16 (2016); R. Jay, 'Guide to the General Data Protection Regulation: a Companion to Data Protection Law and Practice' (Sweet & Maxwell: London, 4nd Revised ed., 2017).

[145] See G. Finocchiaro, 'Intelligenza Artificiale e protezione dei dati personali' *Giurisprudenza Italiana*, 1670-1677 (2019), 1674.

[146] See S. Wachter, B. Mittelstadt and L. Floridi , 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation'

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

2. Ex Post *Explanations, Significant Information and Right to Access*

Legal authors who support the existence of a right to an *ex-post* explanation argue that, despite its non-binding nature[147], Recital 71 would be sufficient to ground the right to explanation, due to the central role of recitals in the interpretation of the provisions of a European Union act.

In addition, it is affirmed that the provisions outlined in Articles 13-14, when specifying that data subjects are entitled to have "*meaningful* information about the logic involved" and also "the *meaning* and intended consequences of such processing", recognize the data subject's right to request an explanation of an algorithmic decision made against him/her.[148] The right to know even "the *meaning* and intended consequences of such processing" is furthermore new, since under the Data Protection Directive, the right to access only included the right to know the logic involved in automated decision-making (Article 12(a)). This addition seems particularly notable, and has been emphazized by those authors who believe that a right to explanation exists (italics added).[149]

7 *International Data Privacy Law*, 2, 76-90 (2017), 83. For a different opinion see See G. Malgieri – G. Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' 7 *International Data Privacy Law*, 4, 243-265 (2017), 255; I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 16.

[147] See A.D. Selbst and J. Powles, "Meaningful information and the right to explanation' 7 International Data Privacy Law, 4, 233-242 (2017); I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 16; B. Goodman and S. Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' 38 *AI Magazine*, 3, 50-57 (2017).

[148] See B. Goodman – S. Flaxman, 'European Union regulations on algorithmic decision-making and a "right to explanation"' 38 *AI Magazine*, 3, 4 (2017), 52; L. Edwards and M. Veale, 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for' 19 *Duke Law & Technology Review*, 1, 19-84 (2017), 46; M. Brkan, n 39 above.

[149] See M.E. Kaminski, 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189 (2019), 21; G. Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2019), 23; E. Falletti, 'Automated decisions and Article No. 22 GDPR of the European Union: an analysis of the right to an "explanation"' *Machine Lawyering* (28 January 2020); R. Messinetti, 'La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Albeit of non-binding value, another strictly legal topic supporting the existence of an *ex post* right of explanation is drawn from the Council of Europe's 2020 Recommendation on AI.[150] These Recommendations on the Human Rights Impact of Algorithmic Systems, in Article 4.3., under the heading "Contestability", stipulate that "Affected individuals and groups should be afforded effective means to contest relevant determinations and decisions. As a necessary precondition, the existence, process, rationale, reasoning and possible outcome of algorithmic systems at individual and collective levels should be explained and clarified in a timely, impartial, easily-readable and accessible manner to individuals whose rights or legitimate interests may be affected, as well as to relevant public authorities. Contestation should include an opportunity to be heard, a thorough review of the decision and the possibility to obtain a non-automated decision. This right may not be waived, and should be affordable and easily enforceable before, during and after deployment, including through the provision of easily accessible contact points and hotlines".[151] Also of importance is the Recommendation CM/Rec(2021)8 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, where widespread references to the right of explanation.[152]

tecnologico e diritto alla spiegazione della decisione automatizzata' *Contratto e impresa*, 3, 861-894 (2019), 875.

[150] Council of Eur., Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems 9, 13 (2020).

[151] Although it is also invoked in support of the existence of a right to an ex-post explanation, less significance seems assumed by 2018 Protocol of Amendment to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981: see Council of Eur., Convention 108+: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 15 (2018). The amending Protocol was meant to update and enhance the Convention by taking into account the new challenges that have emerged regarding the protection of individuals with regard to automated processing of personal data. Among the new features introduced by the protocol there are new rights of individuals with regard to algorithmic decision-making. In particular, Article 9(1)(a) states that "1. Every individual shall have a right: a). not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration". This article has been read as the recognition of a right to contest: see M.E. Kaminski and J.M. Urban, 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189-218 (2019), 1962. However, doubts can be cast on this reading of the rule, which seems rather directed at ensuring that the opinion of the data subject is taken into account: somewhat representing what is the right to express his or her point of view included in Article 22(3).

[152] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Some states have followed these indications and expressly recognized and regulated the right to contest, such as France and Hungary. In France – but limited to administrative decisions – the data controller ensures the control of algorithmic processing and its developments, in order to be able to explain, in detail and in a comprehensible form, to the data subject how the processing was implemented in his/her case.[153] On the other hand, Hungarian law provides – without restriction – for all significant decisions based solely on automated data processing that the controller must inform the data subject of the methods and criteria used in the decision-making mechanism.[154]

The Hungarian law, through its reference to "methods and criteria", also seems to refer to the weighting parameters used for scoring and profiling.[155] On this point, French law is also significant, although perhaps less explicit than Hungarian law, requiring data controllers to provide specific information on the main features of the implementation of algorithmic data processing. These references to national laws will be even more eloquent in the light of what will be laid down regarding the controller's obligations to disclose the weighting of the factors that influenced the decision, and how this information should be disclosed, in aggregate or disaggregated form.

3. *Right to Access and Effective Exercise of the Right to Contest*

However one might legitimately doubt that the scope of application of the information requirements of Articles 13 and 14 extends to recognize the right to receive a detailed explanation of the internal logic followed by the system in the particular case, it is undeniable

States on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[153] Article 10, 2, Loi n° 78-17 du 6 janvier 1978 as amended by Loi n° 2018-493 du 20 juin 2018, 2°: "(…). *Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a étémis en oeuvre à son égard* (…)".

[154] See 2018. évi XXXVIII. Törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról.

[155] See G. Malgieri, 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards"in the national legislations', 35 *Computer Law and Security Review*, 1 (2019), 16-17.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

that, in order to effectively exercise the right to contest under Article 22(3), accurate information is necessary. In this section of the paper, we will address whether the right to access might be the most appropriate solution for this purpose.

Notwithstanding the contrary opinion of those scholars according to which Article 15 would not provide the data subject with new and different rights than those already granted by Articles 13 and 14, it is rightfully stated that if the right to access is exercised after the decision has been taken, the information to be provided would not follow the time constraints of Articles 13(2)(f) and 14(2)(g), and therefore the controller could not limit itself to presenting merely the information available at the beginning of the process.[156]

Further, if the information that the data subject can obtain under Articles 13 and 14 were the same as he is already entitled to under Article 15, the lawmaker would have made the exercise of the right to access conditional on the information not having been received;[157] instead, this requirement is not foreseen, and a reasonable explanation is that the person may have an interest in having more information than he or she has already received or an up-to-date picture.[158] This is consistent with the different function of the two sets of rules: notification and access serve two distinct, albeit interconnected purposes, and create different obligations for data controllers. While Articles 13 and 14 establish "notification obligations" that have to be communicated when personal data are collected or obtained, in order to make the data subject aware of "the importance and consequences" of automated decision-making (even if not exclusively automated), Article 15 introduces the right to access that can be exercised at any

[156] See G. Malgieri – G. Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' 7 *International Data Privacy Law*, 4, 243-265 (2017), 256; I. Mendoza and L. Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20), 16.

[157] Indeed, Article 15 lacks a provision such as Article 13(4), which explicitly provides for such an exception.

[158] Agrees with the assumption that, regarding the content, although the provisions are almost identical, it is necessary to make a distinction between the information due under Articles 13 (2)(f) and 14 (2)(g) and that due as a result of exercising the right to access: E. Troisi, 'AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla intellegibilità dell'algoritmo' *European Journal of Privacy Law & Technologies*, 1, 41-59 (2019), 54.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

time.[159] Accordingly, if the request is made after a decision has been taken, the main features of the processing that must be disclosed to the data subject include the data processed and their source, the processing criteria and their weighting applied to the data subject's situation.[160]

The availability of this amount of information depends thus on how one interprets the legal relationship between the right to access guaranteed by Article 15(1)(h) and the rights guaranteed by Article 22(3) to question an automated decision. This is due to the fact that the scope of information to be provided on the basis of an access claim is only sufficiently "significant" if the data subject is able to exercise the rights ensured by Article 22(3) consciously, accurately and as effectively as possible.[161]

[159] According to what is convincingly argued by G. Comandé, 'Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali' *Danno e Responsabilità*, 2, 33-42 (2022), 147, the expression "and, at least in those cases" contained in Articles 13(2)(f) and 14(2)(g) would not refer only to the cases referred to in Article 22(1)(4), i.e. those exclusively automated, but to "automated decision-making" in general, even if not giving rise to a "solely" automated or non-significant decision. Thus, the obligations to provide the data subject with "significant information about the logic used and the importance and envisaged consequences of such processing" apply generally, to any automated decision-making, even if human intervention was present or concerned a non-significant decision (such as advertising a product I have already purchased). See also F. Bravo, 'Trasparenza del codice sorgente e decisioni automatizzate' *Diritto dell'informazione e dell'informatica*, 4-5, 693-724 (2020), 713, for which the right to access must be interpreted both as the right of the data subject to know the logic of the system's operation, *ex ante*, and as the right to have an explanation of the decision *ex post*.

[160] The weight given by S. Wachter, B. Mittelstadt e L. Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017), 87, to the German case law on SCHUFA of 2014 (see Judgment of the German Federal Court: BGH: Umfang einer von der SCHUFA zu erteilenden Auskunft BGH, Urteil vom 28 January 2014 – VI ZR 156/13 (LG Gießen, AG Gießen) to support their argument that the right to access would be limited seems excessive, because in that case the German Federal Court did not address the question of the extent to which the data subject is entitled to know the logic involved, as the Court excluded that there had been an automated decision.

[161] Important in this respect was the recent BGH judgment, which, for the first time, commented on the scope of the right to access under Article 15(1), adopting a very broad interpretation. In particular, the BGH clearly rejected the argument that access need not be provided if the data subject is already in possession of the information. Article 15 also allows repeated requests, which is why known data are also covered. Furthermore, the German court held that the right to access only achieves its purpose if all processed data are included at the time of access: see German Federal Court of Justice (BGH), 15 June 2021, Case No VI ZR 576/19. The Dutch jurisprudence, on which see E. Falletti, 'Discriminazione algoritmica' (Torino: Giappichelli, 2022), 174, has issued

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

On the question of the connection between Article 15 and the guarantees of Article 22(3) there is an important Austrian question pending before the European Court of Justice.[162]

The European courts are asked to clarify whether the right to access is related to the rights under Article 22(3), insofar as the scope of the information to be provided following a request for access under Article 15(1)(h) appears to be sufficiently "significant "only if the person requesting access is put in a position to exercise those rights in an effective, articulate and foreseeably useful manner. In the context of this question, the Austrian court poses two extremely important questions.

With the first, it asks the European Court of Justice to clarify the relationship between the principle of maximum transparency of information and the protection of trade secrets. In cases involving profiling, should the person entitled to access be provided, even if the existence of a trade secret is alleged, with at least information concerning (1) the data of the person concerned being processed, (2) the components of the algorithm underlying the profiling, in so far as this is necessary for its comprehensibility, and (3) the elements and factors relevant to establishing the correlation between the information being processed and the resulting assessment.

The second question asks the Court of Justice to clarify what content requirements information has to have in order to be considered "significant" under Article 15(1)(h). In particular, the right to access must be interpreted as meaning that "significant information" can only be considered to be that which is so extensive as to enable the person to determine whether the information provided is also true, i.e. whether the information provided formed the basis for the automated decision in question. If the answer is positive, the question arises as to how to proceed whether the accuracy of the information provided by the controller can be verified only if data of third parties are also disclosed. The conflict between the right to access and the protection of third parties' data could be resolved by communicating the data of third parties exclusively to the administrative or judicial authority, with the consequence that they will be the ones to verify whether the data communicated to the data subject are accurate.

a decision taking a different approach, but nevertheless recognizing wide scope to the right to access.

[162] Dun & Bradstreet Austria, Case C-203/22, available at *CURIA - Case information* (europa.eu) (last access 9 March 2023).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

4. *Controller's Obligations and Disaggregated Data*

The question of information and explanations to be provided to the data subject is, however, made more difficult in terms of practical realization by the fact that in business practice data controllers often refuse to comply with requests from data subjects regarding automated decisions – as witnessed by a recent survey[163] –, hiding behind the alleged lack of a legal obligation to do so. They usually limit themselves to general and illustrative statements on how the algorithm works and, at most, on their company policy regarding the implementation of automated devices and the way data is collected, without going into too much detail or providing a complete analytical picture. A reluctance due not so much to technical shortcomings, but to avoid exposing the business logic of data controllers, profit-maximising strategies and other possibly more regrettable behaviors

Actually, the right to be informed of the existence of an automated decision-making, including profiling, and to receive meaningful information on the logic involved, as well as on the importance and expected consequences of such processing for the data subject, goes far beyond a one-sentence overview of how an algorithmic decision-making system works.[164] Data subjects must be given sufficient information to be able to understand what they are consenting to (if consent is the basis legitimizing the decision-making process), or to contest the decision.[165] What Selbst & Powles have argued is to be endorsed, namely that the GDPR's legal standard of meaningful information must at a minimum enable "a data subject to exercise his or her rights under the GDPR and Human Rights Law".[166]

[163] See J. Dexe, U. Franke, K. Söderlund, N. van Berkel, R. Hagensby Jensen, N. Lepinkäinen and J. Vaiste., 'Explaining automated decision-making: a multinational study of the GDPR right to meaningful information' 47 *The Geneva Papers on Risk and Insurance - Issues and Practice*, 669 (2022).

[164] See M.E. Kaminski, 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189 (2019), 211.

[165] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 13: "*Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to.*"; see also at 17, 27, 31.

[166] See A.D. Selbst and J. Powles, 'Meaningful information and the right to explanation' 7 *International Data Privacy Law*, 4, 233-242 (2017), 236.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

A relationship clearly emerges from the text of the GDPR, and then from the WP29 guidelines, between the individual rights granted to the data subject and the kind of personalized transparency that is required. This suggests something interesting about transparency, namely that it is the substance of the underlying legal rights that determines the substance of it. In concrete terms, this translates into the circumstance that if a person has a right against discrimination, he or she should be able to know what factors have been used in a decision. Otherwise, information asymmetries would effectively render the underlying rights null and void.[167]

Equally, Recital 71(2) addresses the issue of factors and means to discover whether discrimination is hidden behind an automated decision, since it does not limit itself to statements of principle, but also requires that the controller "use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, 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 that result in measures having such an effect".

As has been argued by Lagioia, Sartor and Simoncini, this part of the Recital is important to avoid prejudicial and discriminatory decisions. Firstly, because the controller must demonstrate that the input data are accurate, relevant and not taken out of context. It must be demonstrated that the legitimate expectations of the data subject are fulfilled in relation to the purposes for which the data were collected. And this for machine learning systems would concern not only the data subject's data but also the training sets data, since the presence there of bias or discrimination may affect the individual decision.[168]

Regarding what the WP29 guidelines specify about the obligations of data controllers, we can begin by noting that they are not required

[167] See M.E. Kaminski, 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189 (2019), 213.

[168] See F. Lagioia, G. Sartor and A. Simoncini, 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390, 384.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

to provide a complex explanation of the algorithms used or full disclosure of how it works, but one must provide – in ways that are, as far as possible, straightforward and to the point – sufficiently complete 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.".[169] (emphasis added).

In the latter regard, a problem arises with respect to the indication on the weight of the factors that influenced the decision, which if expressed on an aggregate level can make it difficult to detect discrimination.[170] To the extent that data are aggregated, information can only be displayed in groups and as part of a summary, because atomic data from multiple sources are replaced by totals or summary statistics.[171]

[169] See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251, (Oct. 3, 2017, revised Feb. 6, 2018), 1-37, 27. In order to make the information meaningful and understandable, the Committee stresses that real, tangible examples should be given of the kind of effects that are possible. If, hypothetically, an insurance company uses automated decision-making to set car insurance premiums based on the monitoring of customers' driving behavior, to illustrate the meaning and expected consequences of such processing it should inform that dangerous driving can lead to higher insurance payments through an app to give advice on how to improve these habits and consequently how to reduce insurance premiums; similar visual techniques could be used to explain how a past decision was made.

[170] See S. Ruggeri, S. Hajian, F. Kamiran, and X. Zhang, 'Anti-discrimination Analysis Using Privacy Attack Strategies' (Conference: Machine Learning and Knowledge Discovery in Databases - European Conference, ECML PKDD 2014, DOI: 10.1007/978-3-662-44851-9_44); L. Franck, 'Sub Article 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person', in P. Gola ed, *Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar* (German: Verlag C. H. Beck, 2nd ed., 2018), 390-405.

[171] Separating the information collected into smaller units is useful for highlighting underlying trends and patterns. This contributes to a better understanding of a situation, as data are grouped by dimension, such as age, gender, geographical area, education, ethnicity or other socio-economic variables. The classification of data on the basis of personal characteristics is, among other things, in line with the EU General Data Protection Regulation, which, as mentioned above, allows the legitimate collection and processing of "special categories of personal data" (Article 9). In fact, it is widely believed that only the collection of data at a disaggregated level enables the promotion of human rights, because it allows for a deeper analysis of the data to identify inequalities. This is also the reason why the UN General Assembly has recognized data disaggregation as a useful means of identifying discrimination, which refers to laws, policies or practices that appear neutral on the surface, but in reality treat certain population groups less favorably without reasonable justification. See United Nations A/70/335, General Assembly, *Combating racism, racial discrimination, xenophobia and related intolerance*

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

There are ways to detect discrimination even from data sets expressed in aggregate form, but apart from the real risk of violating the privacy of other data subjects, it is very difficult to ascertain which affiliations have contributed most to the algorithm's results if the weight of the factors taken into account for decision-making is given at an aggregate level.[172] But aside from the real risk of violating the privacy of other data subjects,[173] it is very difficult to ascertain which affiliations contributed most to the output of the algorithm if the weight of the factors taken into account for the decision-making are provided on an aggregated level.[174]

and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, 20 August 2015, at § 34 https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/A.70.335.pdf (last access 25 March 2023). See also, United Nations, Economic and Social Council, *Report of the Inter-Agency and Expert Group on Sustainable Development Goal Indicators*, March 2016. https://unstats.un.org/unsd/statcom/47th-session/documents/2016-2-IAEG-SDGs-Rev1-E.pdf (last access 25 March 2023); United Nations, *Overview of standards for data disaggregation*, June 2018, https://unstats.un.org/sdgs/files/Overview%20of%20Standards%20for%20Data%20Disaggregation.pdf (last access 25 March 2023); UN Human Rights Office, *A human rights-based approach to data leaving no one behind in the 2030 agenda for sustainable development*, https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf (last access 25 March 2023).

[172] See J. Kleinberg, J. Ludwigb, S. Mullainathanc, and C.R. Sunstein, 'Algorithms as discrimination detectors' 117 *Proceedings of the National Academy of Sciences*, 48, 30096–30100 (Dec 2020); see also European Union Agency for Fundamental Rights, #BigData: Discrimination in data-supported decision making, 29 May 2018, available at https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making (last access 25 March 2023), 8; see P. Adler et al., *Auditing Black-box Models for Indirect Influence*, Conference: 2016 IEEE 16th International Conference on Data Mining (ICDM), DOI: 10.1109/ICDM.2016.0011.

[173] When data scientists rely on aggregated data, they cannot access the raw information, but a reconstruction attack is able to partially reconstruct an analytical dataset from aggregated information. Conceptually, the role of a data scientist who wants to draw evidence from an aggregated data set is similar to that of an attacker. This would be particularly important to prove discrimination, but this would risk violating the privacy of others. However, the subject is further explored in the specialized scientific literature to provide additional tools for the discovery of discrimination by the anti-discrimination authority (and not by private counter-interested parties). The aim is to balance respect for privacy and protection against algorithmic discrimination: see, e.g., B.-C Chen, L. Chen, R. Ramakrishnan and D.R. Musicant., 'Learning from Aggregate Views', (22nd International Conference on Data Engineering, ICDE'06), http://dx.doi.org/10.1109/ICDE.2006.86.; Y. Chen and S. Yang, 'Estimating Disaggregate Models Using Aggregate Data through Augmentation of Individual Choice' 44 *Journal of Marketing Research*, 4, 613- 621 (2007); F. Kamiran, I. Žliobait and T. Calders, 'Quantifying explainable discrimination and removing illegal discrimination in automated decision making' 35 *Knowledge and Information Systems*, 613-644 (2013).

[174] See S. Ruggeri et al., 'Anti-discrimination Analysis Using Privacy Attack Strategies'

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

However, the WP29's indication of the weight on an aggregate level seems to be just the minimum requirement necessary to fulfil the legal obligations, and the controller has to disclose the factor weights taken into account by the automated system in a disaggregated form whether this is the only way to comply with transparency and access obligations. After all, the controller's obligations go beyond ensuring compatibility with the Regulation, aiming to strengthen the protection of individuals and their fundamental rights. Even if the measures taken ensure (to a nominal extent) compliance with the Regulation, where necessary to protect the rights and freedoms of data subjects, they need to be further supplemented to ensure maximum effectiveness on the ground.[175]

One obstacle to this, is ensuring the anonymity of third persons. Indeed, disaggregation may lead to the identification or re-identification of data subjects. Hence, disaggregation can be envisaged provided that anonymity is maintained, through pseudonymization and/or other measures.[176]

In this regard, what we discussed earlier about the proposal of the Austrian judges, now before the European Court of Justice, to create a protected box in which third-party data are disclosed to the administrative or judicial authority only, without denying the rights of the data subject to have adequate and relevant information about an automated decision in order to be able to assert his or her rights, if any, becomes relevant. Information that, in concrete terms, should at least cover – even if third-party data or trade secrets are involved – (a) the parameters and input values used to arrive at the assessment; (b) the influence of those parameters and input variables on the calculation of the assessment; (c) information on the origin of the parameters or input variables; (d) explanation of the reason why the person entitled

(Conference: Machine Learning and Knowledge Discovery in Databases - European Conference, ECML PKDD 2014), DOI: 10.1007/978-3-662-44851-9_44.

[175] See the study conducted by A. Bernes, 'Dalla responsabilità civile alla responsabilità sociale d'impresa nella protezione dei dati personali: alla ricerca del rimedio effettivo' *Actualidad Jurídica Iberoamericana*, 18, 658-685 (February 2023), 669.

[176] Data aggregation may also have a similar effect to anonymization, in that individual data with personally identifiable details are combined and replaced with a summary representing a group as a whole. Aggregated data is usually represented in a table, with columns representing sensitive attributes such as gender or age, and to which is added another column representing the head count for a combination of these attributes. Companies collect aggregated data for a variety of reasons, firstly because it provides a similar effect to anonymization – although more and more studies are showing that even aggregated data can be traced back to the original data – and secondly because it can for example be used by marketing teams to personalize messaging or offers.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

to access has been assigned a specific score and clarification of the meaning associated with that score; (e) elucidation of the implications of that assessment, listing the categories of profiles, as well as providing an explanation of the rating associated with each of those categories.[177]

III. *Remedies and Sanctions*

The recognition of a right cannot be separated from an adequate framework of remedies and sanctions to ensure its observance. The logic of the compensation and liability rights derives precisely from the universally recognized principle of law "*ubi jus, ibi remedium*", which also underlies the analytical system of remedies and sanctions contained in particular in Chapters VI and VIII of the General Data Protection Regulation.[178]

The GDPR's sanctioning and compensatory framework, despite some uncertainties and hesitations, if exercised correctly by the supervisory authorities and interpreted in a finalistic manner by the experts, can serve not only as a deterrent against the aforementioned malpractices of data controllers failure to address data subjects' requests for clarification or supplying trivial information, but also to guarantee pecuniary and non-pecuniary compensatory protection to the individual affected by a discriminatory automated decision or otherwise not in accordance with the criteria of the Regulation.

1. *Data Controller's Refusal to Provide Significant Information. Legal Instruments of Coercion in the GDPR*

We have ascertained that data controllers are required to meet a high standard of completeness and analyticity in their disclosures,

[177] The problem actually becomes more complex for those computer systems that adapt to user behavior and the environment around them. "Online" machine learning systems can update their prediction model after each decision, incorporating each new observation as part of their training data. With respect to them, we also need to know how and when they interacted or will interact with their environment. See J.A. Kroll, J. Huey, S. Barocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson and H. Yu, 'Accountable Algorithms' 165, *University of Pennsylvania Law Review*, 633-705 (2017), 660.

[178] See G. Zanfir- Fortuna, 'Article 82', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 1160-1179, 1162.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

which shall allow the data subject to enable him/her to exercise the right to contest the automated-decision. Now we need to find out whether there are legal means to sanction (and thus to induce) the data controller to provide accurate and revealing information, as empirical research has shown usually happens (see § II, 4).

Let us take a closer look at the system of remedies, responsibilities and penalties of the EU Regulation 2016/679, which is based on the principle of accountability of data controllers expressed in particular in Articles 5(2), 24 and 32. Accountability implies that controllers are required to take active measures to implement the Regulation (see Articles 24-25, in particular, and the entire Chapter IV). It is up to the controllers to decide for themselves the modalities, guarantees and limits of the processing of personal data – in accordance with the provisions of the law and in the light of certain specific criteria laid down in the Regulation – and the onus is on them to prove that the processing is carried out in accordance with its provisions.

In the context of remedies, the right of any data subject who considers that the processing of his or her personal data infringes his or her rights as a result of a breach of the Regulation to lodge a complaint with a supervisory authority or a judicial authority stands out (Articles 77 and 79). Notwithstanding after the recent pronouncement of the ECJ organizations may do so also without a mandate (see § I, 4.1.), the data subject has the possibility to instruct a non-profit body to file the complaint on his/her behalf, to exercise his/her rights under Articles 77, 78 and 79 and to claim compensation under Article 82, where provided for by the law of the Member State (see Recital 142 and Article 80).[179]

Finally, as regards the penalty system, the GDPR has provided for a whole series of breaches of the Regulation sanctioned by administrative fines imposed by national supervisory authorities with effective, proportionate and dissuasive effect. Moreover, it leaves to the Member States the possibility of establishing other sanctions for violations not subject to fines, which concretely consist in the

[179] That the provision in Article 80 of the Regulation constitutes a proper class action in privacy matters has not always been entirely clear. Part of the legal doctrine has excluded, in fact, that the intervention of the bodies under art. 80 can be construed as a genuine class action aimed at protecting personal data: see A. Candini, 'Gli strumenti di tutela', in G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali* (Bologna: Zanichelli, 2017), 569-594, 589. However, most are of the opinion that Article 80 has thus opened the doors of personal data protection to class action: see C. Irti, 'Consenso "negoziato" e circolazione dei dati personali' (Torino: Giappichelli, 2021), 199.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

possibility for each country to provide for infringements punishable by detention alongside administrative fines (Articles 83 and 84). Punishable conduct also includes infringement of the provisions in Articles 12 to 22 concerning the rights of data subjects, with a penalty of up to 20,000,000 EUR or, for undertakings, up to 4 % of the total annual worldwide turnover of the preceding financial year, whichever is higher (Article 83)(5)(b).[180]

In the light of this framework, we have to wonder what the controller is up against if he/she avoids the specific questions of the data subject or provides incomplete or insufficient information.

In this respect, the data subject may lodge a complaint with the supervisory authority, requesting the Data Protection Supervisor to (a) warn or admonish the controller or processor that the processing operations are likely to violate, or have violated, the relevant provisions in force; (b) order the controller to comply with requests to exercise the rights referred to in Articles 15 to 22 of the Regulation and/or to bring the processing operations into line with the relevant provisions; (c) impose a temporary or definitive restriction on the processing, including a ban on processing. The data subject may also appeal to the judicial authority where the controller has an establishment or, alternatively, to the courts of the Member State where he or she has his or her habitual residence, either directly (instead of the supervisory authority) or after the supervisory authority's response if he or she is not satisfied with it (see Recital 141 and Article 79 of the GDPR and, for the Italian framework, Article 140-bis of the Privacy Code added by Article 13 of Legislative Decree No 101 of 10 August 2018).[181]

[180] Limited to Italian scholarship, a commentary on this legal framework can be found in E. Palmerini, 'Responsabilità da trattamento illecito dei dati personali', in E. Navarretta ed, *Codice della responsabilità civile* (Milano: Giuffrè, 2021), 2466-2508; V. Cuffaro, R. D'Orazio and V. Ricciuto eds, 'I dati personali nel diritto europeo' (Giappichelli: Torino, 2019); R. Panetta ed, 'Circolazione e protezione dei dati personali, tra liberà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)' (Milano: Giuffrè, 2019); G.M. Riccio, G. Scorza and E. Bellisario eds, '*GDPR e normativa privacy. Commentario*' (Milano: Giuffré, 2018); G. Finocchiaro ed, 'Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali' (Bologna: Zanichelli, 2017).

[181] In the Italian legal system, due to the double track system of protection (judicial jurisdiction and national data protection authority), the data subject could appeal to both the general court and the data protection body. See for more details G. Costantino, 'La tutela giurisdizionale dei diritti al trattamento dei dati personali' *Studi di diritto processuale civile in onore di Giuseppe Tarzia*, I, 2265-2302 (2005); G. Carullo, 'Trattamento di dati

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

In addition to these measures (or instead of them, depending on the circumstances of each individual case),[182] the Supervisory Authority may impose an administrative fine pursuant to Article 83. In this regard, the controller risks being fined heavily because he or she does not respect the data subject's rights. In particular, the data subject faces a violation of his or her rights to transparency, legibility and accessibility of the automated decision (Articles 12-15) and is prevented from exercising his or her rights enshrined in Article 22(3). Indeed, if data subjects do not have sufficient information, they cannot know whether they have suffered a legitimate negative response or a discrimination-based decision and cannot therefore exercise their right to contest. The exercise of this right in fact requires a cumulative assessment of a whole series of questions, according at least to the scheme drawn up by Bayamlioglu.[183]

This fine may be increased according to the controller's willingness or unwillingness to cooperate with the authorities to remedy the breach and mitigate its possible negative effects; the seriousness of its failure; any previous relevant breach; the number of data subjects affected; and the categories of personal data concerned by the breach. Regard must also be paid – if sanctions follow the measures referred to in Article 58(2) – to whether those measures have been complied with, so as to attain a greater deterrent effect (see Article 83(2) and for instance Article 164-bis(4) of the Italian privacy code).[184]

Along with these sanctions and actions, the data subject could also claim compensation for the damage suffered as a result of the breach of

personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato' *Rivista Italiana di Diritto Pubblico Comunitario*, 1-2, 131-163 (2020).

[182] We cannot exclude the possibility that the controller does not actually have this information, either because he or she has negligently lost it or not stored it or for other reasons.

[183] See E. Bayamlioglu, 'Contesting Automated Decisions' *European Data Protection Law Review*, 4, 433-446 (2018), 445.

[184] We have already mentioned the cases of food delivery applications decided by the Italian Data Protection Authority: Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. - 10 giugno 2021 [9675440], in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9675440* (last access 24 March 2023); Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 July 2021, in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994* (last access 24 March 2023). In that case, among the various unlawful activities found, there was also the failure to take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject as provided for in Article 22(3). Violation due to the lack of transparency on the functioning of the assignment algorithm.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

the Regulation if he or she proves that the violation resulted in material or immaterial damage.

2. *Breach of Information Obligations and Unfair Damage*

Obligations to provide information and access to personal data are functional to the exercise of the data subject's rights and the activation of the remedies granted by law. [185]

The data controller is obliged to "facilitate" the exercise of the data subject's rights set out in Articles 15-22, according to what Article 12(2) expressly states. Without going back over what has been stated above, but only to link up with what will be discussed below, by exercising the right to access the data subject is granted the power to find out about the existence of an automated decision-making, including profiling, and to obtain significant information about the logic used and the relevance and consequences of such processing for him/her (Article 15(1)(h)).

This premise is necessary in order to ascertain whether the data controller's failure to (adequately) comply with the data subject's request for more information on the automated decision-making constitutes damage compensable under Article 82 GDPR: a provision that attributes to "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.".

A first obstacle in this respect might be the difficulty of framing the position of the person requesting disclosure in a subjective legal situation worthy of protection. It could be argued, in fact, that since what is being complained of in this case is neither the refusal to provide information per se nor the discriminatory decision, but the non-disclosure of significant information, the data subject has merely an instrumental position that does not constitute an entitlement.

[185] See F. Piraino, 'I "diritti dell'interessato" nel regolamento generale sulla protezione dei dati personali', in R. Caterina ed, 'GDPR tra novità e discontinuità', *Giurisprudenza italiana*, Sezione monografica, 2789 (2019); F. Casilai, 'I diritti dell'interessato', in V. Cuffaro, R. D'Orazio e V. Ricciuto eds, *I dati personali nel diritto europeo* (Torino: Giappichelli), (2019), 336; A.B. Gambino and M. Siracusa, 'Sub art. 15', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 306.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Except that GDPR Article 82 adheres to a liability regime that does not meet the requirement of unfairness of damage in the twofold sense of damage generated "*non iure*" (i.e. in the absence of justificatory causes), and "*contra ius*" (i.e. harming a position or interest protected by law), along the lines of the Italian tradition.[186]

To be more precise, the liability paradigm of Article 82 GDPR, coming from the German tradition,[187] adheres to a liability model that makes the unfairness of the damage coincide with the violation of the provisions of the Regulation,[188] according to a scheme that, moreover, is not alien to the Italian legal system: just think of the formulation that receives compensation for damages resulting from a crime, where the author of a criminal offence is required to compensate the financial or non-financial damage that has resulted without requiring a further qualification of unfairness thereof.[189]

[186] In the opposite direction, where the violation, in order to be relevant from the point of view of civil liability, must entail an injury to a legal position that affects the personal sphere of the individual: S. Sica, 'Art. 82', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 893; E. Palmerini, '*Responsabilità da trattamento illecito dei dati personali*', in E. Navarretta, *Codice della responsabilità civile* (Milano: Giuffrè, 2021), 2479, 2482; S. Serravalle, 'Il danno da trattamento dei dati personali nel GDPR' (Napoli: Edizioni Scientifiche Italiane, 2020), 47; partially diverges C. Camardi, 'Note critiche in tema di danno da illecito trattamento dei dati personali' *www.juscivile.it*, 3, 786-811 (2020), 804.

[187] See § 823, Abs. 2, BGB.

[188] See the Opinion of Advocate General M. Campos Sánchez-Bordona, of 6 October 2022, in Case C-300/21 - Österreichische Post (Préjudice moral lié au traitement de données personnelles), which we will discuss later in the text. In particular, see § 86 of the Conclusions where it states, "Article 82 of the GDPR does not lay down any condition other than the infringement of its provisions where this leads to any person suffering material or non-material damage. On the specific calculation of the amount of compensation for that damage, the GDPR does not provide any guidance for national courts.".

[189] See C. Castronovo, 'Responsabilità civile' (Milano: Giuffrè, 2018), 219; C. Scognamiglio, 'Ingiustizia del danno e tecniche attributive di tutela aquiliana' *Nuova giurisprudenza civile commentata*, 2014, II, 353, 358. Scognamiglio rightly points out that the requirement of the injustice of the damage posed by Article 2043 of the Civil Code cannot be "skipped" through the protective norm approach, unless there is an express provision for the compensability of the damage regardless of any investigation into the existence and consistency of a hypothetically injured legal situation (as does happen in the context of the aforementioned Article 185 of the Criminal Code or in the context of the provision of Article 872 of the Civil Code). But in the case at hand here, this limitation does not apply because the provision, Article 82 GDPR, does not respond to the logic of the Italian legal system and therefore must be interpreted autonomously, and not in the light of the internal approach of Italian Civil Code.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

In order to deny the compensability of a harm consisting in the lack of significant information provided on the automated decision-making, it could be argued that the obligation under Article 15(1)(h) is a general obligation of result, so that it does not require compliance also with a qualitative-behavioral standard. However, as has been shown at the end of a thorough and persuasive analysis, the information obligations contained in the GDPR are hardly ever confined merely to prescribing the information to be provided by the data controller to the data subject, since in addition to the result they usually also demand compliance with appropriate conduct.[190] Central to this is the provision in Article 12(1), according to which the data controller is obliged to take appropriate measures to provide the data subject with all the information about the processing referred to in Articles 13 and 14 and the notices referred to in Articles 15-22 in a concise, transparent, intelligible and easily accessible form, using plain and intelligible language.[191]

The data controller, relying on Article 82(3), could exonerate itself from liability by demonstrating that "it is not in any way responsible for the event giving rise to the damage", which in concrete terms could translate into demonstrating that it had taken those "appropriate measures" required by Article 12(1) to provide the data subject with the information referred to in Articles 13 and 14 and the communications referred to in Articles 15-22.

The solution depends on how one understands the effort that must be made by the owner to free himself from liability and is directly related to how the criterion of imputation of liability under Article 82(3) is understood. In fact, if one interprets this rule as requiring an event unrelated to the typical business risk (strict liability or no-fault liability), the data subject must require the controller to take into account all possible variables and all the precautions made available by technology.[192]

[190] See U. Salanitro, 'Illecito trattamento di dati personali e risarcimento del danno. Verso un sistema europeo della responsabilità civile?' *Rivista di diritto civile*, 2023, being published.

[191] Expressly admits the compensability of damage consisting in the violation of the data subject's sphere of information: F. Bilotta, 'La responsabilità civile nel trattamento dei dati personali', in R. Panetta eds, *Circolazione dei dati personali tra libertà e regole del mercato* (Milano: Giuffrè, 2019), 445-468, 464, who consistently denies that contrary arguments can be drawn from Italian courts, as the interpretation of European rules cannot be bound to respect national dogmatics.

[192] See, among others, S. Sica, 'Art. 82', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 893, which requires the demonstration of a third fact giving rise to the damage, endowed with

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

If, on the other hand, this rule is understood as a demonstration of the absence of fault (subjective fault liability), the standard of diligence depends (and thus it becomes relevant inquiring into the extent of diligence that may be required) on the level of effort that may be demanded in connection with that particular processing activity. [193] And, but let it be stated only in passing, the level of diligence required by Article 15(1)(h) does not seem to go as far as the adoption of the most sophisticated measures and the most technologically accurate tools, as established in relation to other obligations, except where the automated decision-making is based on profiling. [194]

As a matter of fact, the debate is reconciled - and the two ways of understanding the rule of Article 82(3) end up leading to substantive results that are not dissimilar overall – if the automated decision-making includes (and is based on) profiling.

the characteristics of unforeseeability and inevitability proper to fortuitous events and force majeure; C. Camardi, 'Note critiche in tema di danno da illecito trattamento dei dati personali' *www.juscivile.it*, 3, 786-811 (2020), 795, which expresses its position in terms of strict liability as a 'dangerous' undertakings, even according to a non-national but European reading of Article 82; B. Van Alsenoy, 'Data Protection Law in the EU: Roles, Responsibilities and Liability' (Cambridge: Intersentia, 2019), 273, 282; F. Bilotta, 'La responsabilità civile nel trattamento dei dati personali', in R. Panetta eds, *Circolazione dei dati personali tra libertà e regole del mercato* (Milano: Giuffrè, 2019), 445-468, 461.

[193] See, among others, A. Hellgardt, 'Die Schadensersatzhaftung für Datenschutzverstösse im System des unionalen Haftungsrechts' *ZEuP*, 2022, 7, 25; M. Gambini, 'Responsabilità e risarcimento nel trattamento dei dati personali', in V. Cuffaro, R. D'Orazio and V. Ricciuto, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 1017, 1048; R. Caterina and S. Thobani, 'Il diritto al risarcimento dei danni' *Giurisprudenza italiana*, 2019, 2805, 2807; D. Barbierato, 'Trattamento dei dati personali e nuova responsabilità civile' *Responsabilità civile e previdenza*, 2019, 2151-2159, 2157; R. Senigaglia, 'Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità informazione e trasparenza nell'ordine della dignità personale' *Nuove leggi civili commentate*, 2017, 1023-1061, 1060.

[194] See the difference in the wording between, on the one hand, the already mentioned provision in Article 12(1), and, on the other hand, Article 32, on the measures to be taken to ensure security of processing, where it reads "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate" (follows the analytical indication of a series of concrete measures).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

3. *Data Protection Impact Assessment and Damage Imputation Criteria*

Data Protection Impact Assessment (DPIA) is a procedure to describe the processing, to assess its necessity and proportionality, and to manage any risks to data subjects' rights and freedoms arising from the processing. Article 35(1) states that "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.".

This is one of the main innovations of the GDPR with respect to the DPD, which goes hand in hand with the principle of accountability (on which the Regulation is based and without which the DPIA would not have been conceivable). While it was previously necessary to request prior authorization from the Supervisory Authority, the GDPR now places the burden of carrying out the analysis of risks to data subjects' freedoms and rights arising from processing directly on the controller. Where there are high risks to the data subjects' freedoms and rights inherent in the processing, the data controller is required to identify the specific measures required to mitigate or eliminate those risks. [195]

If the data controller fails to identify appropriate measures to eliminate or mitigate the risk, he must consult the supervisory authority (so-called prior consultation or prior checking).[196] The evaluation

[195] GDPR's data protection impact assessment finds its seedbed in the impact assessments that have been employed for decades in many regulatory fields to assess (the impact of) risks raised by a specific technology or within a specific context. See E. Kosta, 'Article 35', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 668-679, 668, where references are made to impact assessments developed in the 1960s to study the consequences of technological inventions, environmental impact assessments and privacy impact assessments first carried out in the 1990s in Canada, New Zealand and Australia, initially by public sector bodies and later by industry, as a means of safeguarding privacy interests and as a tool to display accountability.

[196] The supervisory authority normally has a period of eight weeks to give its opinion in writing, which may be extended for a further six weeks, and may also order the prohibition of processing (Article 36(2)). Normally the authority intervenes *ex post*, indicating further measures to be implemented, up to and including possibly admonishing the controller or prohibiting processing. Although part of the doctrine is in the direction of considering that

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

provided by the Supervisory Authority within the scope of prior consultation seems to be considered binding and to be implemented.[197]

The impact assessment is mandatory only for particular processing operations, listed in Article 35(2), among which it stands out for its importance in our discussion, when "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" (Article 35(1)a)).

According to these provisions, and in order to facilitate the task of

prior consultation is not prior authorisation, the controller is not in breach of the GDPR by initiating the processing operation in the absence of written advice received within the above-mentioned time limits: see R. Torino, 'La valutazione d'impatto (Data Protection Impact Assessment)', in V. Cuffaro, R. D'Orazio and V. Ricciuto, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 876; C. Alvarez Rigaudias and A. Spina, 'Article 36', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 665-679, 686. It is reasonable to consider that if the data controller carries out a processing operation that he himself identifies as dangerous because it is carried out in the absence of appropriate measures to prevent the risk, the processing operation must be considered to be in breach of the Regulation, and therefore unlawful for the purposes of civil liability: see U. Salanitro, 'Illecito trattamento di dati personali e risarcimento del danno. Verso un sistema europeo della responsabilità civile?' *Rivista di diritto civile*, 2023, being published. Indeed, it would be absurd to allow the implementation or continuation of a treatment that has been assessed as dangerous and, therefore, in violation of the rights and freedoms of the data subjects (without prejudice to the possibility for the data controller to request the intervention of the authority after the eight weeks have elapsed, and without prejudice to the possibility of charging the authority for the loss of earnings suffered due to the impossibility to carry out the processing in the meantime).

[197] This opinion seems to be shared by: F. Bilotta, 'La responsabilità civile nel trattamento dei dati personali', in R. Panetta eds, *Circolazione dei dati personali tra libertà e regole del mercato* (Milano: Giuffrè, 2019), 445-468, 467, which considers that if damage should occur despite the observance and execution of the measures indicated by the Supervisory Authority, the data controller would not be held liable. Spread a different opinion: C. Alvarez Rigaudias and A. Spina, 'Article 36', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press), 665-679, 686, in order to comply with Article 23, which requires the existence of a specific law protecting vested interests in order to allow the restriction of some provisions of the GDPR (in particular, transparency duties or data protection rights). But by deeming prior consultation binding, one does not restrict the rights of data subjects, but rather guarantees their freedom exercise. Nor can the endeavor to maintain an adequate margin of autonomy for the accountability principle go so far as to legitimise choices that are oriented towards the erosion of rights and freedoms.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

data controllers and processors, the Italian Data Protection Authority has produced a list of processing operations subject to the requirement of impact assessment (similar positions have been taken by data protection authorities in other jurisdictions). The various types of processing also include those concerning:

1) Evaluative or scoring processing carried out on a large scale, profiling, predictive activities;

2) Automated processing operations whose purpose is to take decisions which produce legal effects or which are likely to have a significant effect on the data subject, such as preventing the proper exercise of a right or the use of a good or service or the continuation of an existing contract;

3) Processing operations involving the systematic use of data for the purpose of observing, monitoring or controlling data subjects, including online or App-based data collection, processing of unique identifiers capable of identifying users of information society services, and processing of metadata e.g. in telecommunications, banking, etc;

4) Large-scale processing of extremely personal data, including data related to family or private life, or affecting the exercise of fundamental rights (such as location data) or the breach of which has a serious impact on the data subject's daily life.[198]

Consequently, whenever processing (even if not "solely" automated) gives rise to a profiling activity aimed at taking decisions that produce legal effects or are likely to have a significant impact on the data subject, a data protection impact assessment is mandatory, since the processing is characterized by an extremely high level of risk. For this reason, the data controller's liability attribution regime also undergoes a change, ceasing to depend on the level of diligence that can be expected, and becoming more strictly based on the adoption, or not, only of those measures capable of bringing the risk below the threshold of tolerability: if the prior consultation ex Article 36 has been requested, also by assessing compliance with the indications issued by the Supervisory Authority.[199] The controller, therefore, is

[198] See 'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679' - 11 October 2018 [9058979].

[199] Consistent with what we have argued about the autonomy of the compensation system of Article 82 from the Member States' compensation systems, the controller's exemption from liability should not be understood as coinciding only with the demonstration of a third factor at the origin of the damage, endowed with the characteristics

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

"objectively" liable for the damage without the possibility of freeing himself from this imputation,[200] unless he proves that all technological measures available on the market or indicated by the Supervisory Authority to reduce or avoid the production of the damage have been adopted.[201]

The solution is fully in line with the accountability principle, the prevailing and imminent principle throughout the Regulation, also in the area of damages,[202] insofar as it is expressed in Articles 24 and 32, where this graduation of the incisiveness of the measures according to the risk that the processing brings is evident. According to Article 24, the controller is obliged to implement "appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation", according to "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons".

Similarly, the subsequent Article 32 places an obligation on the controller and the processor to adopt "appropriate technical and organisational measures to ensure a level of security appropriate to the risk", according to "the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons".

Consequently, the higher the risk, the more stringent the countermeasures must be, thus reducing the margin of proof of the controller to exonerate him from liability: in the case of automated decisions based on profiling, the measures that the controller has to show to have adopted to exonerate himself from liability are all and

of unforeseeability and inevitability typical of (only) fortuitous event and force majeure, but as the demonstration of the adoption of all measures technically available on the market or indicated by the Supervisory Authority to reduce or exclude the damage.

[200] In reality, this is not a strict liability, because it remains a liability based on fault, only that the scope of the controller's liberating proof is reduced to showing that he took all (and only) the technologically existing measures to avoid the (that) damage.

[201] Differently S. Sica, 'Art. 82', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 893, he advocates an interpretation of Article 82 in conjunction with Article 2050 of the Italian Civil Code, a provision regulating liability for the exercise of dangerous activities, under the aegis of which the legal framework of the unlawful processing of personal data was brought under the previous DPD regime (also for the exemptions of liability which, according to the prevailing doctrine and Italian courts, are essentially summarized in the fortuitous event and force majeure).

[202] See B. Van Alsenoy, 'Data Protection Law in the EU: Roles, Responsibilities and Liability' (Cambridge: Intersentia, 2019), 273, 283.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

only those that, in relation to that specific type of risk (but also in relation to the state of the art at the time),[203] could have prevented or reduced the damage.[204]

4. *Compensation for Material and Non-Material Damages Arising from Automatic Discriminatory Decisions*

Stating that the Regulation's violation is the only and necessary condition for the liability under Article 82 means that in order to give protection to interests harmed by discriminatory conduct falling outside those expressly forbidden by law (because not founded on protected grounds or manifesting itself in non-statutory contexts) it is not necessary to bring them under the protective umbrella of the right to data protection.[205] It is sufficient that such decisions were decisively based on

[203] It is supported by A. Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection' 32 *Computer Law & Security Review*, 2, 238-255 (2016), 163, that even such measures, according at least to Recitals 84 and 94, would not go beyond the criterion of professional diligence, having to take account of the technologies and costs of implementation. But U. Salanitro's objection seems more than appropriate that in this very case it would be reasonable to concede, denying interpretative relevance on this profile to the recitals, that the rule may demand stricter measures because of the risk these treatments carry: see U. Salanitro, 'Illecito trattamento di dati personali e risarcimento del danno. Verso un sistema europeo della responsabilità civile?' *Rivista di diritto civile*, 2023, being published.

[204] See C. Camardi, 'Note critiche in tema di danno da illecito trattamento dei dati personali' *www.juscivile.it*, 3, 786-811 (2020), 795, 797; U. Salanitro, 'Illecito trattamento di dati personali e risarcimento del danno. Verso un sistema europeo della responsabilità civile?' *Rivista di diritto civile*, 2023, being published; R. Caterina and S. Thobani, 'Il diritto al risarcimento dei danni' *Giurisprudenza italiana*, 2019, 2805, 2807, the latter, however, while arguing that if there is a system designed to oblige data controllers to adopt a series of measures and tools to ensure the lawfulness of the processing and to demonstrate compliance with the regulatory requirements, it would be inconsistent not to accept that such a demonstration is appropriate to exclude liability, adopt a criterion of liability for presumed and qualified fault that appears insensitive to the seriousness of the risk generated by the processing, the substance of which appears to be the same for all types of processing; A. Bernes, 'Dalla responsabilità civile alla responsabilità sociale d'impresa nella protezione dei dati personali: alla ricerca del rimedio effettivo' *Actualidad Jurídica Iberoamericana*, 18, 658-685 (February 2023), 667, which identifies GDPR conformity also in the compliance of the measures taken with all other technically possible and proportionate capable of preventing the harmful event complained by the data subject.

[205] This seems to be how E. Palmerini, 'Responsabilità da trattamento illecito dei dati personali', in E. Navarretta ed, *Codice della responsabilità civile* (Milano: Giuffrè, 2021), 2466-2508, 2488, approaches the issue, i.e. by including in the concept of the right to the protection

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

data subject's personality aspects inconsistent with the purpose of such automated decision-making to give rise to civil liability and thus open the door to compensation for pecuniary and non-pecuniary damage.[206]

However, the premise that a violation of the Regulation is sufficient to amount to liability under Article 82 is not conclusive in order to obtain compensation for any damage resulting from the adoption of an automated discriminatory decision. Apart from what we have discussed regarding the controller's exemption from liability (Article 82(3)), there is an obligation to provide evidence on the data subject's side in order to be effectively compensated. Nor does the condition of non-compliance with the "appropriate technical and organisational measures to avoid discriminatory effects" lead automatically to compensation. Beyond the (proof of) the violation of a provision of the Regulation, the alleged harm and the existence of a causal link between the unlawful conduct and the complained harm (which must also be proven) is also required.[207]

The harm is not in *re ipsa* but must be proved by the injured party.[208]

In addition to being verbatim from Article 82 - if compensability had arisen directly from the Regulation's violation, there would have been no need to indicate the damage, moreover specified in its material and non-material declination - [209] this demonstration's necessity has been

of personal data the discrimination produced by conduct that does not fall within the list of those expressly prohibited or that is based on aspects of the data subject that are not protected by statute, and which would therefore otherwise remain unprotected, providing them with a remedy via the argument that they are the product of violations of the data protection right.

[206] It seems to support the view that the Regulation gives rise to a notion of unlawfulness that coincides with the violation of any provision: G. Versaci, 'La contrattualizzazione dei dati personali dei consumatori' (Napoli: Edizioni Scientifiche Italiane, 2020), 209.

[207] It is argued that Article 82(3) implies a presumption of the causal link, so that once the existence of the damage is proved by the data subject, the burden of proof is reversed, to his benefit: see C. Iorio, 'Appunti sulla responsabilità da trattamento dei dati' *Actualidad Jurídica Iberoamericana*, 18, 1148-1171 (February 2023), 1157. But this is a line of reasoning that draws its argument from Article 1218 of the Italian Civil Code, as expressly stated, and which cannot therefore be directly transferred to a rule that is peculiarly (and with logics) European. What is different, is to make an argument for the possibility of applying facilities to the data subject test, but on the basis of European liability law principles and rationale, as will be discussed later in the text.

[208] See, however, the jurisprudential position of some German courts that do not consider the allegation of damage necessary, the loss of control over the data is sufficient: B. Paal, 'DS-GVO Art. 82 Höhe des Ersatzes immaterieller Schädennach', Beck-online, NJW 2022, 3673.

[209] See furthermore Recital 85, where an analytical indication of the damage that unlawful processing may entail.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

upheld by Italian judges (whose judgement, in the European approach that has been given to this work, is however not very conclusive) [210] but also by other EU judicial bodies. [211]

Proof of material damage resulting from a discriminatory decision can be easy to prove: just consider, among many possible examples, the evidence of a failure to grant economic support, such as an inclusion income, to which the applicant was entitled and which the computer system refused because of the applicant's ethnicity or a characteristic unrelated to the performance. Given the breach proof, then it will only be a matter of calculating the monthly payments in respect of which the economic benefit was denied.

[210] Corte di Cassazione, 2.7.2021, no 18783; 20.8.2020, no 17383; 8.1.2019, no 207 and 25.1.2017, no 1931, all available at *www.italgiureweb.it*. However, there is no shortage of contrary positions, even among judges, in favor of recognizing compensation for non-material damage even in the absence of proof of a harmful consequence, the mere ascertainment of the tort being enough. Unlike material damage (Article 2043 civil code), in the Italian system immaterial damage is typical, i.e., it is only compensable in cases provided for by law (Article 2059 civil code), as is the case here with Article 82 GDPR. The complex issue can be examined in the legal literature following the entry into force of the GDPR: see S. Serravalle, 'Il danno da trattamento dei dati personali nel GDPR' (Napoli: Edizioni Scientifiche Italiane, 2020), 67; E. Tosi, 'Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale' (Milano: Giuffrè, 2019), 240; R. Caterina and S. Thobani, 'Il diritto al risarcimento dei danni' *Giurisprudenza italiana*, 2805 (2019); S. Thobani, 'Il danno non patrimoniale da trattamento di dati tra danno presunto e danno evento', *Giurisprudenza italiana*, 1, 43-46 (2019); S. Sica, 'La responsabilità civile per il trattamento illecito dei dati personali', in A. Mantelero and D. Poletti eds, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa: Pacini Editore, 2018), 161-175; M. Gambini, 'Principio di responsabilità e responsabilità aquiliana' (Napoli: Edizioni Scientifiche Italiane, 2018), 65; G. Ramaccioni, 'La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria' (Napoli: Jovene Editore, 2017), 165; G. Agrifoglio, 'Risarcimento e quantificazione del danno da lesione della privacy: dal danno alla persona al danno alla personalità', *Europa e diritto privato*, 1265 (2017); A. Mantelero, 'Responsabilità e rischio nel Regolamento UE 2016/679' *Nuove leggi civili commentate*, 1, 144-164 (2017).

[211] See the above mentioned Court of Justice of the European Union, 28 April 2022, C-319/201, Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e V., available at *https://curia.europa.eu/juris/document/document.jsf?text=&docid=258485&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=205442* (last access 6 August 2022), which opened up the possibility for associations to take action against acts detrimental to the protection of personal data without a mandate from the data subject, and without the need to 'prove an actual damage suffered by the data subject, in a given situation, as a result of the infringement of his rights' (paragraph 72).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

More problems concern the proof of immaterial damage, due to the difficulty of proving intangible harm in its substance.

Just recently, on 6 October 2022, Advocate General of the Court of Justice M. Campos Sánchez-Bordona delivered his Opinion in Case C-300/21, concerning the compensability of non-pecuniary damage as a consequence of a violation of the right to the protection of personal data. The case originated in Austria, where a publishing company had collected personal data on the political preferences of a group of citizens. In particular, using an algorithm, the company identified addresses of target groups for party election advertising. One of the addressees of the communications complained to the court that he had not given his consent to the processing of his data and claimed equitable damages for non-pecuniary loss suffered as a result of the unlawful processing. The Austrian Supreme Court asked the European Court of Justice to give a preliminary ruling on whether the mere infringement of the GDPR provisions gave rise to an automatic right to compensation, regardless of whether damage had been suffered.

In his conclusions, the Advocate General noted that for the purposes of awarding damages for harm suffered by a person as a result of a GDPR breach, a mere rule violation is not sufficient if it is not accompanied by evidence of the relevant harm, whether pecuniary or non-pecuniary. If the legislator, as in other areas of EU law, had intended that the breach of a rule should automatically give rise to a right to compensation, it would have so provided. This is not the case with regard to the GDPR, which contains rules relating to proof, or having direct consequences on proof, such as Article 82(3) (4). To reason otherwise, according to the Advocate General, would attribute to compensation a punitive nature that it does not have, and that is instead left to criminal penalties and administrative fines.[212]

Closely linked to the issue of proof of non-pecuniary damage is the necessary existence of a minimum threshold of importance of the prejudicial consequences for the data subject, below which he or she would not be compensated. In fact, to compensate insubstantial damage, devoid of significance and that does not go over and above the irritation, anger, frustration or other negative feelings that the unlawful

[212] See the Opinion of Advocate General M. Campos Sánchez-Bordona, of 6 October 2022, in Case C-300/21 - Österreichische Post (Préjudice moral lié au traitement de données personnelles).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

processing of personal data may provoke would mean reintroducing the configurability of compensation without damage.[213]

As regards the causation requirement, it should be interpreted, at least if one pursues a conception closer to what might be a native European civil law system of liability, as meaning that the conduct complained off must be the decisive cause of the damage. Thus, damages that cannot be decisively attributed to the conduct of the controllers, in breach of the Regulation's obligations, are to be excluded, as this fault factor might be too remote in relation to the intervening liability of other parties or arising from other factors. [214]

This strict way of qualifying both proof of harm and proof of causation might discourage recourse to protection or consider it hardly practicable, but this is not the case. After all, it is not necessary for the alleged victim to provide direct and complete proof of discrimination. Indeed, especially where objective criteria are used for the imputation of the tort, as in the case of the GDPR, an interpretation in conformity with EU law should read the rules as a relative legal presumption. [215] By distributing the burden of proof, it protects the weaker party of the relationship who finds it more difficult to provide evidence.[216]

[213] See also the importance that seems to be played, despite the contrary opinion of the Advocate General, by Recitals 75 and 85, which contain an illustrative list of damages ending with an open-ended clause that seems to limit compensable damages to those that are "significant". Agreeably attaches importance to them U. Salanitro, 'Illecito trattamento di dati personali e risarcimento del danno. Verso un sistema europeo della responsabilità civile?' *Rivista di diritto civile*, 2023, being published. And again see C. Camardi, 'Note critiche in tema di danno da illecito trattamento dei dati personali' *www.juscivile.it*, 3, 786-811 (2020), 795, 805, according to which "the data subject may request the cessation of the unlawful conduct on the ground that it infringes his right to control the circulation of personal data, but he should not also be able to claim compensation for non-pecuniary damage unless there is a nuisance, a personal inconvenience that is at least significant".

[214] See T-40/15 - ASPLA e Armando Álvarez / Unione europea, especially points 108 and 109, where other important case law references can be found.

[215] See G. Carapezza Figlia, 'Il divieto di discriminazione quale limite all'autonomia contrattuale' *Rivista di diritto civile*, 6, 1387-1418 (2015), 1412-1413. The author argues from the case law of the European Court of Justice that in discrimination disputes, it is up to the victim to prove the facts from which the existence of direct or indirect discrimination can be presumed. Once these facts are proven, it is then up to the defendant to show that there has been no violation of the principle of non-discrimination

[216] In the context of anti-discrimination protection, the European Court of Justice, in the case of an employer who had failed to comply with requests for information from a rejected applicant (who had assumed that he had been refused because of his nationality), held that a denial of any access to information may constitute grounds for a presumption of direct or indirect discrimination: see C-415/10 – Meister.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

The same Court of Justice of the European Union, with regard to the causal link, has opened up the possibility of considering certain factual elements as subsisting, if they are accompanied by sufficiently serious, precise and concordant findings, when ascertaining the etiological link between a certain event and the occurrence of a given harmful consequence.[217]

[217] See C-621/15, N. W et al. v. Sanofi Pasteur MSD SNC et al., 21 June 2017.

ISBN 978-88-495-5249-2
© Edizioni Scientifiche Italiane

Conclusions

In the light of the analysis carried out we can state that Article 22 is well suited to address the discriminatory threats inherent in automated decisions, both when they target characteristics protected by anti-discrimination law as well as when they target unprotected characteristics. Even when it comes to statutorily unpredicted characteristics, such as owning a pet, being a video gamer, or frequenting a social network, if the decision-making system's algorithm functionally attaches decisive weight to them and makes the granting or not of the underlying benefit or service depend on them, then that automated decision is illegitimate, because data subjects are to be assessed in an objective manner and only for characteristics closely related to the good or service concerned.

Article 22 is a regulatory tool that has the ability to counter discriminatory algorithmic decisions, especially if one interprets it as a general prohibition preventing the controller from taking decisions unless there are legal exceptions. Although the rather high threshold of significance excludes decisions from which no relevant consequences result, this does not in itself lead to the exclusion of potentially discriminatory practices regarding access to goods and/or services, especially when they are based on the "profiling" of personal aspects such as "preferences or interests (…) or behaviour".

The worthiness of Article 22 in counteracting discriminatory/differentiating practices is also mirrored by the interpretation of the human contribution to the decision, which, if it is merely nominal or lacks the necessary competences and powers to modify algorithmic decisions, does not exclude the application of the prohibition and the corresponding legal framework.

Nor does the breadth and width of the exceptions to the prohibition invalidate the overall soundness of these conclusions. Because consent is backed by strong safeguards, as is the contractual exemption, which expressly has on its side the criterion of necessity, and the European law or a Member State's law derogation must provide for elevated measures to protect the rights, freedoms and legitimate interests of the

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

data subject. In the case of algorithmic decisions based on sensitive data, these strengthenings become even more stringent, to the point of denying room for the contractual exception, envisaging areas in which not even the data subject himself can derogate from the prohibition, and in any case requiring the application of even stricter measures, which should be no less effective than those listed in Article 22(3) ("right to obtain human intervention on the part of the controller, to express one's point of view, to contest the decision").

As regards the right to contest the automated decision and the information needed to exercise it, even if a right of explanation is not expressly recognized, the exercise of the right to access may allow the collection of information enabling the data subject to exercise his or her right to contest appropriately. The right to access is functional, and may be exercised even after the decision has reached the person concerned, to the exercise of the data subject's rights and legitimate interests and to the triggering of remedies provided by law. We have shown that experts have come up with solutions which make it possible to reconcile respect for the privacy of third parties with the right of the data subject to know on what basis he has been assessed, by limiting access to data, as well as input and output for the relevant decisions, to the judiciary or the supervisory authority.

A right, if not accompanied by a system of sanctions and remedies, does not really exist. That is why the GDPR accompanies these rights with a whole series of remedies and sanctions entrusted mainly to national supervisory authorities, which, despite some uncertainty and hesitation, act as a deterrent to data controllers' refusal to disclose meaningful information.

Flanking this system of sanctions is a remedial framework based on Article 82, which responds to its own logic and not that of national jurisdictions. A system in which the violation of the Regulation, including its rules of principle, is already sufficient to determine damage compensation, without further reference to other conditions or requirements to make it unfair. And in which the imputation criterion of Article 82(3) fluctuates according to the risk introduced into the legal-economic system by the type of processing at stake: the higher the risk, the fewer the defences that the controller can put forward, so much so as to be reduced to proof of having adopted all and only those measures suitable to avoid the damage produced by a discriminatory decision when an impact assessment has been carried out (Article 35). Of course, this does not exclude the data subject from

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

having to prove the infringment of the Regulation, the damage (both material and significant immaterial) resulting therefrom, and the causal link. But the EU-born civil liability system, with which Article 82 has also to be interpreted, already contains test concessions to facilitate a person affected by discriminatory decisions, which can also be tailored to non-protected grounds.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Bibliography

Adler P. et al., 'Auditing Black-box Models for Indirect Influence' (Conference: 2016 IEEE 16th International Conference on Data Mining, ICDM).

Alloway T., 'BIG data: Credit where credit's due' *Financial Times* (February 4, 2015).

Alpa G. ed, 'Diritto e intelligenza artificiale' (Pisa: Pacini Editore, 2020).

Alvarez Rigaudias C. and Spina A., 'Article 36', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), 665-679.

Amato S., 'Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie' (Torino: Giappichelli, 2020).

Ammannati L. – Greco G.L., 'Il credit scoring alla prova dell'intelligenza artificiale', in U. Ruffolo ed, *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (Torino: Giappichelli, 2021), 373-386.

Astone A., 'Autodeterminazione nei dati e sistemi A.I.' *Contratto e impresa*, 2, 429-448 (2022).

Astromskė K., Peičius E. and Astromskis P., 'Ethical and legal challenges of informed consent applying artificial intelligence in medical diagnostic consultations' 36 *AI & Society*, 509-520 (2021),

Avitabile L., 'Il diritto davanti all'algoritmo' *Rivista italiana per le scienze giuridiche*, 8, 315-327 (2017).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Baratta R., 'Complexity of EU law in the domestic implementing process', in *19th Quality of legislation seminar "EU legislative drafting: Views from those applying EU law in the Member States"*, European Commission service juridique – quality of legislation team (Brussels, 2014).

Barfield W. – Pagallo U., 'Research Handbook on the Law of Artificial Intelligence', (Cheltenham: Edward Elgar Publishing, 2018).

Barocas S. – Selbst A., 'Big Data's Disparate Impact' 104 *California Law Review*, 3, 671-732 (2016).

Bayamlioglu E., 'Contesting Automated Decisions' *European Data Protection Law Review*, 4, 433-446 (2018).

Baldini D., 'Article 22 GDPR and prohibition of discrimination. An outdated provision?' *CiberLaws* (August 20, 2019).

Barba V., 'Principio di eguaglianza e tutela dei contraenti', in M. Cavallaro, F. Romeo, E. Bivona and M. Lazzara eds, *Sui mobili confini del diritto. Scritti in onore di Massimo Paradiso*, II, (Torino: Giappichelli, 2022), 333-383.

Barbierato D., 'Trattamento dei dati personali e nuova responsabilità civile' *Responsabilità civile e previdenza*, 2151-2159 (2019).

Battelli E., 'Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi' *Corriere giuridico*, 12, 1517-1526 (2019).

Bell M., 'Anti-discrimination law and the European Union' (Oxford: Oxford University Press, 2002).

Bernes A., 'Dalla responsabilità civile alla responsabilità sociale d'impresa nella protezione dei dati personali: alla ricerca del rimedio effettivo' *Actualidad Jurídica Iberoamericana*, 18, 658-685 (2023).

Biferali G., 'Big data e valutazione del merito creditizio per l'accesso al peer to peer lending' 34 *Diritto dell'informazione e dell'informatica*, 3, 487-509 (2018).

Bird & Bird, 'Profiling and Automated Decision-Taking' (*www.twobirds.com*)

Bilotta F., 'La responsabilità civile nel trattamento dei dati personali', in R. Panetta ed, *Circolazione dei dati personali tra libertà e regole del mercato* (Milano: Giuffrè, 2019), 445-468.

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Bravo F., 'Trasparenza del codice sorgente e decisioni automatizzate' *Diritto dell'informazione e dell'informatica*, 4-5, 693-724 (2020).

Britz G., 'Freie enfaltung durch selbstdarstellung' (Tübingen: Mohr Siebeck, 2007).

Brkan M., 'Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond' 27 *International Journal of Law and Information Technology*, 2, 91–121 (2019).

Brownsword R., 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality', in S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne, S. Nouwt eds, *Reinventing data protection?* (Dordrecht: Springer, 2009), 83-110.

Buttarelli G., 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit European Data Protection Supervisor', 11 April 2017 (*edps.europa.eu*).

Bygrave L., 'Article 22', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), 530-532.

Bygrave L., 'Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' 17 *Computer Law & Security Review*, 1, 17-24 (2017).

Caia A., 'Sub Article 22', in G.M. Riccio, G. Sforza and E. Bellisario eds, *GDPR e Normativa Privacy Commentario*, I (Milano: Wolters Kluwer, 2018), 219-229.

Camardi C., 'Note critiche in tema di danno da illecito trattamento dei dati personali' *www.juscivile.it*, 3, 786-811 (2020).

Candini A., 'Gli strumenti di tutela', in G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali* (Bologna: Zanichelli, 2017), 569-594.

Carapezza Figlia G., 'Il divieto di discriminazione quale limite all'autonomia contrattuale' *Rivista di diritto civile*, 6, 1387-1418 (2015).

Carullo G., 'Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato' *Rivista Italiana di Diritto Pubblico Comunitario*, 1-2, 131-163 (2020).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Casilai F., 'I diritti dell'interessato', in V. Cuffaro, R. D'Orazio and V. Ricciuto eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 327-348.

Castronovo C., 'Responsabilità civile' (Milano: Giuffrè, 2018).

Caterina R. and Thobani S., 'Il diritto al risarcimento dei danni' *Giurisprudenza italiana*, 2805-2810 (2019).

Checchini B., 'Discriminazione contrattuale e dignità della persona' (Torino: Giappichelli, 2019).

Chen B.-C, Chen L., Ramakrishnan R. and Musicant D.R., 'Learning from Aggregate Views', in *22nd International Conference on Data Engineering* (ICDE'06).

Chen Y. – Yang S., 'Estimating Disaggregate Models Using Aggregate Data through Augmentation of Individual Choice' 44 *Journal of Marketing Research*, 4, 613- 621 (2007).

Chopin I., Farkas L. and Germaine C., 'Ethnic origin and disability data collection in Europe – Comparing discrimination', Migration Policy Group for Open Society Foundations (2014).

Comandé G., 'Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali' *Danno e Responsabilità*, 2, 2022, 33-42 (2022).

Costantino G., 'La tutela giurisdizionale dei diritti al trattamento dei dati personali', in *Studi di diritto processuale civile in onore di Giuseppe Tarzia*, I, 2265-2302 (2005).

Crawford K., 'Think Again: Big Data' *Foreign Pol'y* (May 10, 2013).

D'Ippolito G., 'Processi decisionali automatizzati nel settore assicurativo. Un'indagine preliminare' *MediaLaws*.

D'Adda A., 'Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilita` civile ed iniziative di diritto europeo' *Rivista di diritto civile*, 5, 805-837 (2022).

De Felippe Reis B. and Caxambu Graminho V.M., 'A inteligência artificial no recrutamento de trabalhadores: o caso amazon analisado sob a *ótica* dos direitos fundamentais', in *XVI Seminário Internacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea* (2019).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

De Franceschi A., 'Sub Article 4', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 153-176.

Dexe J., Franke U., Söderlund K., van Berkel N., Hagensby Jensen R., Lepinkäinen N. and Vaiste J., 'Explaining automated decision-making: a multinational study of the GDPR right to meaningful information' *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47, 669–697 (2022).

Di Ciommo F., 'Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio', in V. Cuffaro, R. D'Orazio and V. Ricciuto eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 353-390.

Di Rosa G., 'Quali regole per i sistemi automatizzati "intelligenti"?' *Rivista di diritto civile*, 5, 823-853 (2021).

Donadio G., 'Responsabilità da violazione del divieto di discriminazione', in E. Navarretta, *Codice della responsabilità civile* (Milano: Giuffrè, 2021), 2509-2520.

Doshi-Velez et al., 'Accountability of AI under the law: The role of explanation' (Berkman Center Research Publication Forthcoming: Harvard Public Law Working Paper, 2017).

Eder N., 'Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling', in M. Ebers and M. Cantero Gamito eds, *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges*, I (Cham: Springer, 2021), 23-47.

Edwards L. and Veale M., 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' 16 *IEEE Security & Privacy*, 3, 46–54 (2018).

Edwards L. and Veale M., 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for' 19 *Duke Law & Technology Review*, 1, 19-84 (2017).

European Commission High-Level Expert Group on Artificial Intelligence, 'Ethics guidelines for trustworthy AI' (2019).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

European Union Agency for Fundamental Rights, 'Bias in Algorithms artificial intelligence and discrimination' (Luxembourg: Publications Office of the European Union, 2022).

Falletti E., 'Discriminazione algoritmica' (Torino: Giappichelli, 2022).

Falletti E., 'Automated decisions and Article No. 22 GDPR of the European Union: an analysis of the right to an "explanation"' *Machine Lawyering* (28 January 2020).

Falletti E., 'Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche' 36 *Diritto dell'informazione e dell'informatica*, 2, 169-206 (2020).

Ferrari I., Becker D. and Wolkart E.N., 'Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos' 107 *Revista dos Tribunais, São Paulo*, 107, 995, 635-655 (2018).

Ferretti F., 'The Legal Framework of Consumer Credit Bureaus and Credit Scoring in the European Union: Pitfalls and Challenges—Overindebtedness, Responsible Lending, Market Integration, and Fundamental Rights' XLVI *University Law Review*, 3, 791-828 (2013).

Finlayson-Brown J. and Catharina G., 'German Court asks CJEU to clarify whether calculating consumer credit scores falls within the scope of automated decision-making under GDPR' (*www.allenovery.com*).

Finocchiaro G. ed, 'Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali' (Bologna: Zanichelli, 2017).

Finocchiaro G., 'Intelligenza Artificiale e protezione dei dati personali' *Giurisprudenza Italiana*, 1670-1677 (2019).

Fondrieschi A.F., 'A Fragile Right: The Value of Civil Law Categories and New Forms of Protection in Algorithmic Data Processing under the GDPR' *Osservatorio del diritto civile e commerciale*, 2, 435-469 (2019).

Franck L., 'Sub Article 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person', in P. Gola ed, *Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar*, 2. Auflage (München: C.H. Beck), 390-405 (2018).

Franzoni M., 'Lesione dei diritti della persona, tutela della privacy e in-

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

telligenza artificiale', in U. Ruffolo ed, *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (Torino: Giappichelli, 2021), 339-355.

Gabrielli G. and Ruffolo U. eds, 'Intelligenza artificiale e diritto' *Giurisprudenza italiana*, Sezione Monografica, 7 (2019).

Gambini M., 'Principio di responsabilità e responsabilità aquiliana' (Napoli: Edizioni Scientifiche Italiane, 2018).

Gambini M., 'Responsabilità e risarcimento nel trattamento dei dati personali', in V. Cuffaro, R. D'Orazio and V. Ricciuto, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 1017.

Gambino A.B. and Siracusa M., 'Sub art. 15', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 306.

Geburczyk F., 'Automated administrative decision-making under the influence of the GDPR – Early reflections and upcoming challenges' 41 *Computer law & Security Review*, 105538 (2021).

Gellert R., De Vries K., De Hert P. and Gutwirth S., 'A Comparative Analysis of Anti-Discrimination and Data Protection Legislations', in B. Custers, T. Calders, B. Schermer and T. Zarsky eds, *Discrimination and Privacy in the Information Society* (Cham: Springer), 61-89 (2013).

Gentili A., 'Il principio di non discriminazione nei rapporti civili' 27 *Rivista critica di diritto privato*, 2, 207-231 (2009).

Gerards J. and Xenidis R., 'Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law' (Luxembourg: Publications Office of the European Union, 2021).

Gini C., 'I pericoli della Statistica', Roma (1939).

Goodman B. and Flaxman S., 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' 28 *AI Magazine*, 3, 50-57 (2017).

Gitti G., 'Dall'autonomia regolamentare e autoritativa alla automazione della decisione robotica' *Tecnologie e diritto*, 1, 113-127 (2020).

Hacker P., 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' 55 *Common Market Law Review*, 4, 1143 – 1185 (2018).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Hellgardt A., 'Die Schadensersatzhaftung für Datenschutzverstösse im System des unionalen Haftungsrechts' *ZEuP*, 7-43 (2022).

Hildebrandt M., 'The Dawn of a Critical Transparency Right for the Profiling Era', in J. Bus et al eds, *Digital Enlightenment Yearbook*, IOS Press, 41-56 (2012).

Hoeren T. and Niehoff M., 'Artificial intelligence in medical diagnoses and the right to explanation', *Eur. Data Prot. L. Rev.*, 4, 308-319 (2018).

Hurley M. and Adebayo J., 'Credit Scoring in The Era of Big Data' 18 *Yale Journal of Law & Technology*, 148-216 (2016).

Iaselli M., 'Sanzioni e responsabilità in ambito GDPR' (Milano: Giuffrè, 2019).

Ingold D. and Soper S., 'Amazon Doesn't Consider the Race of Its Customers. Should It?' (April 21, 2016).

Iorio C., 'Appunti sulla responsabilità da trattamento dei dati' *Actualidad Jurídica Iberoamericana*, 18, 1148-1171 (2023).

Irti C., 'Consenso "negoziato" e circolazione dei dati personali' (Torino: Giappichelli, 2021).

Jay R., 'Guide to the General Data Protection Regulation: a Companion to Data Protection Law and Practice', 4th Revised, (Sweet & Maxwell: London, 2017).

Kamarinou D., Millard C. and Singh J., 'Machine Learning with Personal Data' (Queen Mary School of Law Legal Studies Research Paper), 247 (2016).

Kaminski M.E. and Urban J.M. , 'The right to contest AI' 121 *Columbia Law Review*, 7, 1957-2048 (2021).

Kaminski M.E., 'The Right to Explanation, Explained' 34 *Berkeley Technology Law Journal*, 189-218 (2019)

Kamiran F., Žliobaitė I. and Calders T., 'Quantifying explainable discrimination and removing illegal discrimination in automated decision making' 35 *Knowledge and Information Systems*, 613-644 (2013).

Kim P.T., 'Data-Driven Discrimination at Work' 58 *William & Mary Law Review*, 3, 857-936 (2017).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Kleinberg J., Ludwigb J., Mullainathanc S., and Sunstein C.R., 'Algorithms as discrimination detectors' 117 *Proceedings of the National Academy of Sciences*, 48, 30096–30100 (2020).

Klimas T. and Vaiciukaite J., 'The Law of Recitals in European Community Legislation' 15 *Journal of International & Comparative Law*, 61-39 (2008).

Knutson J., 'Credit Scoring in the Insurance Industry: Discrimination or Good Business?' 15 *Loyola Consumer Law Review*, 4, 315-329 (2003).

Kobie N., 'The Complicated Truth About China's Social Credit System', *WIRED UK* (June 7, 2019).

Korff D., 'New Challenges to Data Protection Study - Country Report: Germany', European Commission DG Justice, Freedom and Security (2010).

Kosta E., 'Article 35', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), 668-679.

Kroll J., Huey J., Barocas S., Edward W. Felten, J.R. Reidenberg, D.G. Robinson and H. Yu, 'Accountable Algorithms' 165 *University of Pennsylvania Law Review*, 633-705 (2017).

Kuner C., Svantesson D.J.B., Cate F.H., Lynskey O. and Millard C., 'Machine learning with personal data: is data protection law smart enough to meet the challenge?' 7 *International Data Privacy Law*, 1, 1-2 (2017).

Lagioia F. and Sartor G., 'Il sistema COMPAS: algoritmi, previsioni, iniquità', in U. Ruffolo ed, *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (Giappichelli: Torino, 2021), 226-243.

Lagioia F., Sartor G. and Simoncini A., 'Sub Article 22', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 379-390.

Landini S., 'Insurtech: innovation in production, distribution, governance, and supervision in the insurance market' *Assicurazioni*, 3, 433-446 (2021)'.

Langenbucher K., 'Responsible A.I.-based Credit Scoring - A Legal Framework' 31 *European Business Law Review*, 4, 527-572 (2020).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Lanni S., 'Dataquake: intelligenza artificiale e discriminazione del consumatore' *Nuovo diritto civile*, 2, 97-123 (2020).

La Rocca D., 'Le discriminazioni nei contratti di scambio di beni e servizi', in M. Barbera ed, *Il nuovo diritto antidiscriminatorio. Il quadro comunitario e nazionale* (Milano: Giuffré, 2007), 289-341.

Laviola F., 'Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa' *Biolaw Journal*, 3, 389-440 (2020).

Lerman J., 'Big data and its exclusions' 66 *Stanford Law Review Online*, 55-63 (2013).

Liguori L., 'Sub Articles 13-14', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 289-304.

Lohsse S., Schulze R., Staudenmayer D. eds, '*Liability for Artificial Intelligence and the Internet of Things*' (München-Oxford: Nomos, 2019).

Lynskey O., 'General Report Topic 2: The New EU Data Protection Regime', in J. Rijpma ed, *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, The XXIX FIDE Congress in The Hague: Congress Publications, II (Eleven Publishing, 2020), 23-48.

Lyon D., 'Surveillance as social sorting: privacy, risk, and digital discrimination' (Routledge: New York, 2003).

Maffeis D., 'Il contraente e la disparità di trattamento delle controparti' *Rivista di diritto privato*, 281-312 (2006), 281.

Maffeis D., 'Discriminazione (diritto privato)' *Enciclopedia del Diritto*, Annali, IV, (Milano: Giuffrè, 2011), 490-510.

Malgieri G. and Comandé G., 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' 7 *International Data Privacy Law*, 4, 243-265 (2017).

Malgieri G., 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations' 35 *Computer Law and Security Review*, 1-26 (2019).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Manes P., 'Credit scoring assicurativo, machine learning e profilo di rischio: nuove prospettive' *Contratto e impresa*, 469-489 (2021).

Mantelero A., 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection"' 32 *Computer Law & Security Review*, 2, 238-255 (2016).

Mantelero A., 'Responsabilità e rischio nel Regolamento UE 2016/679' *Nuove leggi civili commentate*, I, 144-164 (2017).

Martini M., 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling', in B. Paal and D. Pauly eds, *Datenschutz-Grundverordnung*, 1st edn (Beck-online, 2017), 249-265.

Mendoza I. and Bygrave L., 'The Right not to be Subject to Automated Decisions based on Profiling' (University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20).

Messinetti R., 'La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata' *Contratto e impresa*, 3, 861-894 (2019).

Micklitz W., Pollicino O., Reichman A., Simoncini A., Sartor G. and De Gregorio G. eds, 'Constitutional Challenges in the Algorithmic Society' (Cambridge University Press, 2021).

Morozzo della Rocca P. ed, 'Principio di uguaglianza e divieto di compiere atti discriminatori' (Napoli: Edizioni Scientifiche Italiane, 2002).

Navarretta E., 'Principio di uguaglianza, principio di non discriminazione e contratto' *Rivista di diritto civile*, 3, 547-566 (2014).

Noto La Diega G., 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 1, 3-34 (2018).

Paal B., 'DS-GVO Art. 82 Höhe des Ersatzes immaterieller Schädennach' (Beck-online, NJW 2022), 3673.

Pagallo U., 'Algo-Rhythms. The Beat of the Legal Drum' 31 *Philosophy and Technology*', 4, 507-524 (2018).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Palmerini E., 'Algoritmi e decisioni automatizzate. Tutele esistenti e linee evolutive della regolazione', in L. Efrén Ríos Vega, L. Scaffardi and I. Spigno eds, *I diritti fondamentali nell'era della digital mass surveillance* (Napoli: Napoli: Edizioni Scientifiche Italiane, 2019), 209-244.

Palmerini E., 'Responsabilità da trattamento illecito dei dati personali', in E. Navarretta ed, *Codice della responsabilità civile* (Milano: Giuffrè, 2021), 2466-2508.

Panetta R. ed, 'Circolazione e protezione dei dati personali, tra liberà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)' (Milano: Giuffrè, 2019).

Parisi N. and Urso G., 'I principi di eguaglianza e di non discriminazione nell'ordinamento dell'Unione europea' *Osservatorio sul rispetto dei diritti fondamentali in Europa*, 24 (2011).

Pasquale F., 'The Black Box Society: The Secret Algorithms That Control Money and Information' (Cambridge-London: Harvard University Press, 2015).

Pehrsson E., 'The Meaning of the GDPR Article 22', EU Law Working Papers 31 (Stanford-Vienna Transatlantic Technology Law Forum, 2018), 1–32.

Pellecchia E., 'Privacy, decisioni automatizzate e algoritmi', in E. Tosi ed, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (Milano: Giuffré, 2019), 417-439.

Pellecchia E., 'Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation' *Nuove leggi civili commentate*, 5, 1209 -1235 (2018).

Perlingieri C., 'Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi' *Actualidad Jurídica Iberoamericana*, 12 bis, 836-847 (2020).

Perlingieri P., 'Sul trattamento algoritmico dei dati' *Tecnologie e diritto*, 1, 181-195 (2020).

Piraino F., 'I "diritti dell'interessato" nel regolamento generale sulla protezione dei dati personali', in R. Caterina eds, *GDPR tra novità e discontinuità* (*Giurisprudenza italiana*, 12), 2789-2799 (2019).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Ramaccioni G., 'La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria' (Napoli: Jovene Editore, 2017).

Reddix-Smalls B., 'Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market' 12 *UC Davis Business Law Journal*, 1, 87-124 (2011).

Reilly. M., 'Is Facebook Targeting Ads at Sad Teens?' *MIT Technology Review* (2017).

Resta G., 'Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza' *Politica del diritto*, 2, 199-236 (2019).

Ricci A., 'I diritti dell'interessato', in G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Zanichelli: Bologna, 2017), 179-250.

Riccio G.M., Scorza G. and Bellisario E. eds, 'GDPR e normativa privacy. Commentario' (Milano: Giuffré, 2018).

Rodotà S., 'Elaboratori elettronici e controllo sociale' (Bologna: Zanichelli, 1973).

Rodway S., 'Just How Fair Will Processing Notices Need to Be Under the GDPR' *Privacy & Data Protection*, 16–17 (2016).

Ruffolo U. ed, 'Intelligenza artificiale. Il diritto, i diritti, l'etica' (Milano: Giuffré, 2020).

Ruffolo U. ed, 'XXVI Lezioni di Diritto dell'Intelligenza Artificiale' (Giappichelli: Torino, 2021).

Ruggeri S., Hajian S., Kamiran F., and Zhang X., 'Anti-discrimination Analysis Using Privacy Attack Strategies' (Conference: Machine Learning and Knowledge Discovery in Databases - European Conference, ECML PKDD 2014).

Salanitro U., 'Illecito trattamento di dati personali e risarcimento del danno. Verso un sistema europeo della responsabilità civile?', being published in *Rivista di diritto civile*.

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Salanitro U., 'Intelligenza artificiale e responsabilità: la strategia della Commissione europea' *Rivista di diritto civile*, 6, 1246-1276 (2020).

Sarra C., 'Il diritto di contestazione delle decisioni automatizzate nel GDPR' *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, XII, 33-69 (2019).

Sarra C., 'Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of Contestability by Design' 20 *Global Jurist*, 2 (2020).

Sartor G. and Lagioia F., 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (European Parliamentary Research Service PE 641.530—June 2020).

Sassi O., 'Profilazione e trattamento dei dati personali', in L. Califano and C. Colapietro eds, *Innovazione tecnologica e valore della persona* (Napoli: Editoriale Scientifica, 2017), 573-628.

Savin A., 'Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks' (Paper presented at 7th International Conference Computers, Privacy & Data Protection, Brussels, 2014), 1-15.

Schartum D., 'From facts to decision data: about the factual basis of automated individual decisions' *Scandinavian Studies in Law*, 379-400 (2018).

Schönberger D., 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' 27 *International Journal of Law and Information Technology*, 171-203 (2019).

Schulz S., 'DS-GVO Art. 22 Automatisierte Entscheidungen im Einzelfall', in Peter Gola ed, *Datenschutz-Grundverordnung Vo (EU) 2016/*679, 1st ed., 410–419 (2017).

Scognamiglio C., 'Ingiustizia del danno e tecniche attributive di tutela aquiliana', *Nuova giurisprudenza civile commentata*, II, 353 (2014).

Selbst A.D. and Powles J., 'Meaningful information and the right to explanation' 7 International Data Privacy Law, 4, 233-242 (2017).

Senigaglia R., 'Reg. UE 2016/679 e diritto all'oblio nella comunicazione

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

telematica. Identità informazione e trasparenza nell'ordine della dignità personale' *Nuove leggi civili commentate*, 1023-1061 (2017).

Serravalle S., 'Il danno da trattamento dei dati personali nel GDPR' (Napoli: Edizioni Scientifiche Italiane, 2020).

Sesso Sarti O., 'Profilazione e trattamento dei dati', in L. Califano and C. Colapietro eds, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (Napoli: Editoriale Scientifica, 2017), 573-619.

Sica S., 'La responsabilità civile per il trattamento illecito dei dati personali', in A. Mantelero and D. Poletti eds, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa: Pacini Editore, 2018), 161-175.

Sitzia L., 'Pari dignità e discriminazione' (Napoli: Jovene Editore, 2011).

Spina A., 'New regulation or new medicine: the complex governance of personal data in medicine', 4 *European Data Protection Law Review*, 3, 280-283 (2018).

Stanzione P., 'Data Protection and vulnerability' *European Journal of Privacy Law & Technologies*, 2, 9-14 (2020).

Suksi M., 'Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective' 29 *Artificial Intelligence Law*, 87–110 (2021).

Thiene A., 'Sub Article 9', in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta eds, *Codice della privacy e data protection* (Milano: Giuffrè, 2021), 240-249.

Thobani S., 'Il danno non patrimoniale da trattamento di dati tra danno presunto e danno evento' *Giurisprudenza italiana*, 1, 43-46 (2019).

Tommasi S., 'Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo' 27 *Revista de Direito Brasileira*, 10, 112-129 (2020).

Torino R., 'La valutazione d'impatto (Data Protection Impact Assessment)', in V. Cuffaro, R. D'Orazio and V. Ricciuto eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019), 876.

Tosi E. eds, 'Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy' (Milano: Giuffrè, 2019).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Tosi E., 'Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale' (Milano: Giuffrè, 2019).

Tosoni L., 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation' 11 *International Data Privacy Law*, 2, 145-162 (2021).

Troisi E., 'AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla intellegibilità dell'algoritmo' *European Journal of Privacy Law & Technologies*, 1, 41-59 (2019).

Turner lee N., Resnick P. and Barton G., 'Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms' (May 22, 2019).

Van Alsenoy B., 'Data Protection Law in the EU: Roles, Responsibilities and Liability' (Cambridge: Intersentia, 2019).

Versaci G., 'La contrattualizzazione dei dati personali dei consumatori' (Napoli: Edizioni Scientifiche Italiane, 2020).

Voigt P. and von dem Bussche A. eds, 'The EU General Data Protection Regulation (GDPR): A Practical Guide' (Cham: Springer, 2017).

Volz D., 'Silicon Valley Thinks It Has the Answer to Its Diversity Problem', ATLANTIC (Sept. 26, 2014).

Wachter S., Mittelstadt B., Floridi L., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 2, 76-90 (2017).

Wachter S., 'Affinity profiling and discrimination by association in online behavioral advertising' 35 *Berkeley Technology Law Journal*, 367-430 (2020).

Xenidis R. and Senden L., 'EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination', in U. Bernitz, X. Groussot, J. Paju and S.A. De Vries eds, *General principles of EU law and the EU digital order* (Alphen aan den Rijn: Kluwer Law International), 151-182 (2020).

York J., 'Getting banned from Facebook can have unexpected and professionally devastating consequences' (Quartz, 31 March 2016).

ISBN 978-88-495-5249-2 © Edizioni Scientifiche Italiane

Zanfir- Fortuna G., 'Article 82', in C. Kuner, L. Bygrave, C. Docksey and L. Drechsler eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), 1160-1179.

Zarsky T., 'Transparent predictions' *University of Illinois Law Review*, 4 (Champaign, 2013), 1503-1570.

Zarsky T., 'Understanding discrimination in the scored society' 89 *Washington Law Review*, 1375-1412 (2014).

Zarsky T.Z., 'Incompatible: The GDPR in the Age of Big Data' 47 *Seton Hall Law Review*, 995-1020 (2017).

Zliobaite I. and Custers B., 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models' 24 *Artificial Intelligence and Law*, 2, 183-201 (2016).

Zuddas P., 'Intelligenza artificiale e discriminazioni' in *Consulta Online* (16 March 2020), 1-18.

Zuiderveen Borgesius F.J., 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' 24 *The International Journal of Human Rights*, 10, 1572-1593 (2020).

Zuiderveen Borgesius F.J, 'Discrimination, artificial intelligence, and algorithmic' (Strasbourg: Published by the Directorate General of Democracy of the Council of Europe, 2018).

Zuiderveen Borgesius F.J., 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation' 32 *Computer law & Security Review*, 256–271 (2016).

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

Table of contents

© Edizioni Scientifiche Italiane ISBN 978-88-495-5249-2

ISBN 978-88-495-5249-2

© Edizioni Scientifiche Italiane

LA BUONA STAMPA

Questo volume è stato impresso
nel mese di aprile dell'anno 2023
per le Edizioni Scientifiche Italiane s.p.a., Napoli
Stampato in Italia / Printed in Italy
red./ftc.antdc

Per informazioni ed acquisti

Edizioni Scientifiche Italiane - via Chiatamone, 7 - 80121 Napoli
Tel. 0817645443 - Fax 0817646477
Internet: www.edizioniesi.it