EJLT European Journal of Law and Technology

# Exploring the Synergies between Non-Discrimination and Data Protection: What Role for EU Data Protection Law to Address Intersectional Discrimination?

**Alessandra Calvi***

**Abstract**

In the European Union (EU), anti-discrimination policies have developed an intersectional dimension in recent years, the traditional sectorial approach having neglected differences in terms of gender, race, age, social status, ability, sexual orientation, etc., within a given vulnerable or marginalised group. In parallel, European data protection law has been reformed and enriched with new instruments, including the General Data Protection Regulation (GDPR). Considering that the collection and analysis of information that affects oppression dynamics ground the operationalisation of the intersectionality principle, European data protection law could play a pivotal role in enabling it. Nowadays, the GDPR grants specific protection to some *special categories of data* (which include racial or ethnic origin, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation, etc.) that, to a certain extent, overlap with the information that ought to be disaggregated in accordance with the intersectionality principle. The processing of these data is forbidden unless one of the exceptions foreseen in Article 9(2) GDPR applies.

* Doctoral researcher at the d.pia.lab, LSTS, Vrije Universiteit Brussel; ETIS lab, UMR 8051, CY Cergy Paris Université / ENSEA / CNRS.
This work has been funded under the EUTOPIA PhD co-tutelle programme 2021, award number: EUTOPIA-PhD-2021-0000000127 OZRIFTM5.
I would like to thank for their suggestions, comments and insights: the attendees of the Interdisciplinary Conference on European Advanced Studies (IDEAS) 2022 – (Dis)Integration from an (in)equality perspective (Brussels, May 2022), where an earlier version of this work was presented; the anonymous reviewers of the manuscript; and my colleagues Anastasia Karagianni and Pia Groenewolt.

Yet, are these exceptions framed in a way to promote or undermine intersectionality? And, in general, what is the approach followed by EU data protection law towards intersectional discrimination matters? Building upon a review of data protection and anti-discrimination laws and legal literature, as well as policy documents, this paper will explore the interrelationships between the EU data protection law (in particular, the GDPR) and anti-discrimination law.

After briefly sketching the specific challenges raised by intersectional discrimination, it delves into EU data protection law's understanding thereof, and compares the notions of sensitive data and protected grounds. Considering the importance of processing sensitive data to prevent and address (intersectional) discrimination, it will illustrate the rules applicable to sensitive data. It will then question the sufficiency of some of the exceptions *ex* Article 9(2) GDPR, focusing on the so-called 'substantial public interest exception', deemed the most relevant for intersectionality matters. Finally, it reflects upon the enforcement mechanisms set by the GDPR.

**Keywords: data protection; intersectionality; non-discrimination; special categories of data; substantial public interest**

## 1. Introduction

In 2015, an Amazon recruitment tool was found to rate candidates for technical roles in a manner discriminatory to women. In 2016, in the United States, a software supporting judges with parole decisions was discovered to be more likely to flag African-American than white inmates as being at risk of recidivism. In 2021, an enquiry demonstrated that Dutch tax authorities investigating childcare benefit frauds had for years relied on an algorithm that disproportionately flagged persons with a low income and a migration background as potential fraudsters.[1] These are just a few recent examples of many cases of amplification of human bias performed by allegedly neutral technologies, highlighting increasing interrelationships between the two domains of data protection and discrimination, especially when automated systems are deployed. These overlaps are so significant that equality bodies and Data Protection Authorities (DPAs) across the EU, most notably in France, have (timidly) started to cooperate in an attempt to share expertise and coordinate their actions in the light of the challenges posed by new technologies.[2]

[1] EDRi and others, 'Centring Social Injustice, de-Centring Tech: The Case of the Dutch Child Benefits Scandal'; Li Zhou, 'Is Your Software Racist?' Politico (2 August 2018) <https://www.politico.com/agenda/story/2018/02/07/algorithmic-bias-software-recommendations-000631> (accessed on 12/10/2023); Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women' Reuters (San Francisco, 11 October 2018) <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> (accessed on 12/10/2023).

[2] Janneke Gerards and Raphaële Xenidis, 'Algorithmic Discrimination in Europe – Challenges and Opportunities for Gender Equality and Non-Discrimination Law' (2020); Robin QC Allen and Dee

Both non-discrimination and data protection rights are considered fundamental in the EU and enshrined in primary law, namely the Treaties and the Charter of Fundamental Rights of the European Union (CFR).[3] However, when the two rights are transposed into directives and regulations (secondary law), different approaches to tackling discrimination and data protection issues arise. Admittedly, both anti-discrimination and data protection laws combine proactive approaches (e.g. mainstreaming[4] and by-design[5]) with *ex post* measures (e.g. access to justice and data subjects' rights) for the enforcement of individual rights, and rely on specific administrative bodies.[6] Yet, whereas the GDPR,[7] the cornerstone of EU personal data protection law, aims to be a comprehensive horizontal instrument (Recital 10 GDPR),[8] anti-discrimination law is much more fragmented.[9] Having been conceived essentially to achieve internal market objectives, the legal framework consists of a patchwork of directives,[10]

Masters, 'Regulating for an Equal AI: A New Role for Equality Bodies: Meeting the New Challenges to Equality and Non-Discrimination from Increased Digitalisation and the Use of Artificial Intelligence' (2020).

[3] Charter of Fundamental Rights of the European Union. OJ C 202, 7.6.2016, p. 389–405. As to primary law, the CFR ensures the protection of personal data (Article 8 CFR) and forbids discrimination (Article 21 CFR). Similarly, the Treaty on the Functioning of the European Union (TFEU) refers to the EU aim to combat discrimination in defining and implementing its policies and activities (Article 10 TFEU; see also Article 19 TFEU on legislative procedure; and Article 16 TFEU on the right to personal data protection.

[4] Defined as 'a social justice-led approach to policy making in which equal opportunities principles, strategies and practices are integrated into the every day work of government and public bodies'. Raphaël Gellert and Paul De Hert, 'La Non-Discrimination Comme Réalité Effective En Europe? Réflexions Sur La Procéduralisation Du Droit De L'Égalité Européen' [2011] Revue Belge de Droit Constitutionnel 7.

[5] Aimed at incorporating data protection and fundamental rights considerations throughout the life-cycle of a technology or processing activities. European Data Protection Supervisor, 'Preliminary Opinion on Privacy by Design'.

[6] Raphaël Gellert and others, 'A Comparative Analysis of Anti-Discrimination and Data Protection Legislations' in Bart Custers and others (eds), *Discrimination & Privacy in the Information Society,* (Springer 2013); Gellert and De Hert (n 4).

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 4.5.2016, p. 1–88.

[8] Yet, the panorama is becoming increasingly fragmented by the multiplication data protection rules in different sector (e.g., national rules specifying the GDPR, Law Enforcement Directive, EU rules on EU large-scale databases, e-Privacy, Artificial Intelligence Regulation proposal, Data Governance Act, Data Act Proposal, Open Data Directive).

[9] Gellert and others (n 6).

[10] Namely, the Racial Equality Directive 2000/43/EC, against discrimination on grounds of race and ethnic origin (for access to employment and work conditions, vocational training, social protection and social advantages, education, access to goods and services); the Employment Equality Directive 2000/78/EC against discrimination at work on grounds of religion or belief, disability, age or sexual orientation; the Gender Equality Directive 2006/54/EC on equal treatment for men and women in matters of employment and occupation; the Gender Goods ad Service Directive 2004/113/EC on equal treatment for men and women in the access to and supply of goods and services.

applicable only to certain grounds, individually considered, and in certain situations, whose effectiveness in terms of intersectional discrimination is questionable.[11] In the anti-discrimination directives, the protection on the grounds of race, ethnicity and sex covers only access to employment, welfare systems (specifically, the more limited social security in case of sex) and goods and services, whereas sexual orientation, disability, religion or belief and age are protected only in the context of employment.[12] Over a decade ago, a proposal for a horizontal instrument to tackle discrimination was advanced, but the situation has been on standby since 2009, notwithstanding that President von der Leyen committed to making new anti-discrimination legislation a top priority for 2022 and 2023.[13] Thus, despite several NGOs, expert groups and certain EU bodies and agencies (e.g. the European Institute for Gender Equality) across Europe increasingly warning European legislators of the challenges raised by intersectional discrimination, the situation is frozen.[14]

Can EU data protection law contribute to remedying this stagnation by filling the gaps in EU anti-discrimination law? In spite of criticism for being too technology-driven, not human-centric enough and socially unfocused, it was argued that data protection law could play a pivotal role in both preventing and addressing discrimination,[15] at least, when discrimination is related to a data processing activity (e.g., surveillance, profiling, the inclusion of persons in databases). Indeed, whilst non-discrimination covers a wide range of phenomena (e.g., direct and indirect discrimination, harassment)[16] arising from multiple activities, including data processing, the

[11] Sandra Fredman, 'Intersectional Discrimination in EU Gender Equality and Non-Discrimination Law' (2016); European Union Agency for Fundamental Rights, European Court of Human Rights and Council of Europe, *Handbook on European Non-Discrimination Law* (Publications Office of the European Union 2018); Gellert and De Hert (n 4).

[12] European Union Agency for Fundamental Rights, European Court of Human Rights and Council of Europe (n 11).

[13] Ionel Zamfir, 'Anti-Discrimination Directive' (2023).

[14] Advisory Committee on equal opportunities for women and men, 'Opinion on Intersectionality in Gender Equality Laws, Policies and Practices' 1.

[15] Gellert and others (n 6); Yordanka Ivanova, 'The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI' (2020) 12121 LNCS Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 3; Maria Tzanou, 'The Future of Eu Data Privacy Law: Towards a More Egalitarian Data Privacy' (2020) 7 Journal of International and Comparative Law 449; Frederik J Zuiderveen Borgesius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24 International Journal of Human Rights 1572 <https://doi.org/10.1080/13642987.2020.1743976>; Philipp Hacker, 'Teaching Fairness To Artificial Intelligence: Existing and Novel Strategies' (2018) 55 Common Market Law Review 1143; Laurens Naudts, 'How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2018).

[16] Direct discrimination occurs when a person is treated less favourably than another based directly on a protected ground; indirect discrimination occurs when apparently neutral provisions, criteria or practices determine nevertheless a *de facto* discrimination against a

applicability of data protection law is conditional on (personal) data being processed.[17]

But what about intersectional discrimination, specifically? Does EU data protection law, and particularly the GDPR, provide the right tools to address it? This paper will address these questions building upon a review of data protection and anti-discrimination laws and legal literature, as well as policy documents. Although both legal frameworks are presented, the spotlight will be on data protection instruments. Without neglecting the importance of the Council of Europe and the case law of the European Court of Human Rights, the analysis will cover exclusively EU law and case law.

After briefly sketching the specific challenges raised by intersectional discrimination, I will look into EU data protection law's understanding thereof, and compare the notions of sensitive data and protected grounds. Considering the importance of processing sensitive data to prevent and address (intersectional) discrimination, I will delve into the rules applicable to sensitive data. I will question the sufficiency of some of the exceptions *ex* Article 9(2) GDPR, focusing however on the so-called 'substantial public interest exception', deemed the most relevant for intersectionality matters. Finally, I will reflect upon the enforcement mechanisms set by the GDPR. Although the main object of the analysis will be the GDPR, reference will also be made to the Artificial Intelligence (AI) Regulation proposal[18] (AIR), due to its envisaged role in tackling discrimination, or more precisely, bias performed by automated systems.

## 2. Conceptualising Intersectional Discrimination in EU Law

The EU anti-discrimination legal framework does not expressly acknowledge the existence of intersectional discrimination. Articles 10 and 19 Treaty on the Functioning of the European Union (TFEU)[19] refer to a closed list of protected grounds: sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation, and nationality. In turn, Article 21 CFR provides an open-ended formulation of protected grounds, using wording *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'.[20] Whereas such formulation could in principle encompass cases of intersectional

protected ground; harassment occurs when an unwanted conduct related to a protected ground takes place 'with the purpose or effect of violating the dignity of a person and of creating an intimidating, hostile, degrading, humiliating or offensive environment' Gellert and others (n 6).

[17] ibid.

[18] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final.

[19] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. OJ C 202, 7.6.2016, p. 1–388.

[20] Fredman (n 11).

discrimination, it is important to recall that *ex* Article 51 CFR, the Charter applies only to EU institutions, bodies, offices and agencies and Member States in so far as they are applying EU law 'in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties', meaning that private actors cannot rely on that. Only in very rare, exceptional and limited circumstances, as pointed out by the Court of Justice of the European Union (CJEU) in the cases C-144/04 *Mangold v Helm* and C-414/16 *Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV*, the provisions of the Charter may have horizontal effects.[21] As to the former, [75] and [78] establish that:

> '[…] The principle of non-discrimination on grounds of age must thus be regarded as a general principle of Community law. […] It is the responsibility of the national court to guarantee the full effectiveness of the general principle of non-discrimination in respect of age, setting aside any provision of national law which may conflict with Community law, even where the period prescribed for transposition of that directive has not yet expired.'

As to the latter, [47] states that:

> '[…] the objective of Directive 2000/78 [...] is to lay down a general framework for combating discrimination on the grounds *inter alia* of religion or belief as regards employment and occupation, with a view to putting into effect in the Member States the principle of equal treatment. The directive is thus a specific expression, in the field covered by it, of the general prohibition of discrimination laid down in Article 21 of the Charter.'

Despite the openness of Article 21 CFR, the fragmentation of EU secondary anti-discrimination law, the different scope of the anti-discrimination directives, the fact that exceptions to the rule of not discriminating can be framed differently therein and the impossibility of expanding and combining protected grounds without the intervention of EU legislators jeopardise the conceptualisation and enforcement of intersectional discrimination claims.[22] At the same time, considering that the admissibility and relevance of statistical tests and the elaboration upon comparators (namely, 'an individual or group which has been unjustifiably treated better than an individual or group in a comparable situation'[23]) usually occur on a case-to-case basis, determining *a priori* if something constitutes discrimination proves to be extremely difficult, to the extent that certain authors talk about *contextual equality* when referring to the approach of EU secondary law for discrimination issues.[24] This panorama is further complicated by the fact that to achieve substantial equality,

---

[21] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI' (2021) 41 Computer Law and Security Review 1 <https://doi.org/10.1016/j.clsr.2021.105567>.
[22] Fredman (n 11).
[23] Wachter, Mittelstadt and Russell (n 21) 10.
[24] Wachter, Mittelstadt and Russell (n 21).

Member States are allowed to take *positive actions*, namely to adopt or maintain specific compensatory measures (e.g., quotas at the workplace, access to training) to prevent and compensate disadvantages linked to the protected characteristics.[25]

Elaborated to portray how both gender and race specifically affect the way black women experience discrimination,[26] *intersectional discrimination* refers to a form of discrimination occurring when a person is treated less favourably due to different protected grounds that, inseparably and simultaneously, operate and interact with each other. Therefore, contrary to *multiple discrimination*, where multiple grounds co-exist separately, intersectional discrimination produces a specific type of discrimination.[27] When an employer fails to ensure the accessibility of an office for wheelchair users or to combat the use of misogynist slurs, a female employee with disabilities could be a victim of multiple discriminations. Indeed, the lack of accessibility affects wheelchair users regardless of sex and gender, whilst the misogynist slurs female employees regardless of their abilities.[28] Conversely, rules banning religious face coverings may constitute examples of intersectional discrimination against Muslim women, as it is not possible to separate the grounds of sex and religion for configuring this type of discriminatory situation. The difference with the previous example is rooted in the impossibility of configuring a discriminatory situation without the co-existence of the different protected grounds, considering that neither non-Muslim women nor Muslim men would be affected by these rules. Similarly, adjudicating a lower amount of damages to women victims of negligent gynaecological surgery due to their middle age and status as mothers may constitute intersectional discrimination, since a lower compensation would not be adjudicated to younger women or women without children.[29]

Intersectional discrimination can be performed by automated systems, too – for instance, when facial recognition technologies do not work adequately on female or non-binary black and brown faces.[30] Or when an algorithm designed to rank candidates for university admissions systematically discriminates against women with

[25] Marc De Vos, 'The European Court of Justice and the March towards Substantive Equality in European Union Anti-Discrimination Law' (2020) 20 International Journal of Discrimination and the Law 62.
[26] Kimberle Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics' (1989) 1989 University of Chicago Legal Forum 271; Patricia Hill Collins and others, 'Intersectionality as Critical Social Theory' (2021) 20 Contemporary Political Theory 690.
[27] European Union Agency for Fundamental Rights (FRA), *Handbook on European Non-Discrimination Law* (Publications Office of the European Union 2018).
[28] Center For Intersectional Justice, 'Intersectional Discrimination in Europe: Relevance, Challenges and Way Forward' (2019).
[29] European Union Agency for Fundamental Rights (FRA) (n 27).
[30] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research – Conference on Fairness, Accountability, and Transparency 1; Raphaële Xenidis, 'Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience' (2020) 27 Maastricht Journal of European and Comparative Law 736.

a migration background. Within the computer science community, the discussion on (intersectional) discrimination may be reconducted to the debate on algorithm fairness and bias (defined as 'outcomes which are systematically less favourable to individuals within a particular group and where there is no relevant difference between groups that justifies such harms'[31]) in AI.[32] Although the first computer science works on fairness date back to the mid-1990s, this field took off after 2010, when investigations on discrimination discovery in databases were first carried out, and the approach to fairness through unawareness of protected characteristics proved to be flawed.[33] As a result, multiple technical definitions of AI fairness, corresponding to multiple fairness metrics, reconducted to the two main categories of group fairness and individual fairness, were elaborated.[34] In the past, following a single-axis approach similar to the EU anti-discrimination law, the research in computer science had focused on analysing fairness in relation to single sensitive attributes separately.

Yet, the situation has changed, as such an approach could be misleading. Indeed, automated systems may appear fair with respect to sensitive attributes considered separately, but be unfair with respect to intersectional subgroups.[35] It must be added that, whereas the concepts of bias and fairness are related and to a certain extent overlap with discrimination and equality, they are not identical.[36] Furthermore, what is deemed fair from a legal point of view is in turn influenced by what is deemed fair in the system of ethical values and philosophical beliefs underpinning different societies and their legal systems.[37] In other words, the concept of fairness is domain-specific. Indeed, to put it very simply, an algorithm may be technically fair (because it adheres to one of the many existing fairness metrics) whilst being considered, legally speaking, discriminatory by a court or DPA, which may question the applicability of the said fairness metrics in that specific case. Considering the largely contextual approach towards equality followed by EU anti-discrimination law, automating fairness is currently impossible.[38]

---

[31] Nicol Turner Lee, Paul Resnick and Genie Barton, 'Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms' (2021) para 5 <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms> (accessed on 12/10/2023).

[32] Gerards and Xenidis (n 2).

[33] Toon Calders and others, 'Introduction to The Special Section on Bias and Fairness in AI' (2021) 23 ACM SIGKDD Explorations Newsletter 1.

[34] Karima Makhlouf, Sami Zhioua and Catuscia Palamidessi, 'Machine Learning Fairness Notions: Bridging the Gap with Real-World Applications' <http://arxiv.org/abs/2006.16745>.

[35] Abolfazl Asudeh and others, 'Designing Fair Ranking Schemes' (2019) Proceedings of the ACM SIGMOD International Conference on Management of Data 1259; Ke Yang, Joshua R Loftus and Julia Stoyanovich, 'Causal Intersectionality and Fair Ranking' (2021) 192 Leibniz International Proceedings in Informatics, LIPIcs.

[36] Gerards and Xenidis (n 2).

[37] Alessandra Calvi and Dimitris Kotzinos, 'Enhancing AI Fairness through Impact Assessment in the European Union: A Legal and Computer Science Perspective' (2023) ACM Conference on Fairness, Accountability, and Transparency (FAccT '23) 1229.

[38] Wachter, Mittelstadt and Russell (n 21).

One of the main problems concerning intersectional discrimination regards its enforcement in courts. To date, expressly referring to 'intersectionality' or 'intersectional discrimination' is still taboo in the case law of the CJEU, which accepts the multifaceted connotations of discrimination only implicitly (and partially).[39] For instance, in the case C-443/15 *Parris v Trinity College and others*, concerning the right of a same-sex partner to be entitled to a survivor's pension, the CJEU admitted at [80] that:

> '[…] while discrimination may indeed be based on several of the grounds set out in Article 1 [*religion or belief, disability, age or sexual orientation*] of Directive 2000/78 [*establishing a general framework for equal treatment in employment and occupation]*, there is, however, no new category of discrimination resulting from the combination of more than one of those grounds, such as sexual orientation and age, that may be found to exist where discrimination based on those grounds taken in isolation has not been established.'

The Court further elaborated at [81]:

> 'Consequently, where a national rule creates neither discrimination on the ground of sexual orientation nor discrimination on the ground of age, that rule cannot produce discrimination on the basis of the combination of those two factors.'

Even at a national level, courts tend not to elaborate on issues related to intersectionality.[40] There may be multiple reasonings behind this approach: intersectionality being indissolubly linked with social justice and political activism may sit in stark contrast with the (alleged) neutrality and objectivity of judges.[41] Furthermore, discrimination having been conceived in the EU legal frameworks as a sectorial, single-axis matter (namely, focusing only on one ground at a time),[42] the case law is inevitably influenced by this structure. Other difficulties depend on the challenge of identifying an appropriate comparator for victims of intersectional discrimination.[43] In any event, this represents a huge unresolved gap in the protection of vulnerable and marginalised individuals and groups because it prevents the justiciability of intersectional discrimination claims.

[39] European Union Agency for Fundamental Rights, European Court of Human Rights and Council of Europe (n 11).
[40] Fredman (n 11).
[41] Sirma Bilge, 'Intersectionality Undone: Saving Intersectionality from Feminist Intersectionality Studies' (2013) 10 Du Bois Review Social Science Research on Race 405.
[42] Center For Intersectional Justice (n 28).
[43] Wachter, Mittelstadt and Russell (n 21) 10.

## 3. Interrelations between Data Protection and Non-Discrimination

### 3.1 Discrimination in EU Data Protection Law

The relationship between discrimination and data protection has increasingly been an object of analysis in the past decade, especially due to the widespread use of automated decision systems in many sectors, ranging from recruitment to law enforcement.[44] Considering that the technology and EU legislation trying to regulate it are constantly evolving, and taking into account the first attempts of collaboration between equality bodies and DPAs, it is reasonable to presume the debate will become increasingly significant in the future. Certain authors have highlighted how the protection of the right to non-discrimination is operationalised in the GDPR through the need for the controller – that is, the entity determining objects and purposes of data processing – to respect data processing principles, such as fairness, data minimisation, purpose limitation, and ensure data subjects' rights, such as access, erasure and object to processing.[45] By introducing, e.g., transparency requirements around data collection and use, data protection law could contribute to mitigating information asymmetries between controllers and data subjects and thus mitigate the risks of discrimination.[46] Others focused on the importance of *ex ante* tools, such as data protection impact assessments (DPIAs) and data protection by design, to prevent discrimination.[47] However, these contributions focused on discrimination in general, and not on intersectional discrimination specifically.

In parallel, part of the EU data protection legal framework demonstrates awareness of the interrelations between data processing and discrimination, an advancement considering that the former Data Protection Directive,[48] the predecessor of the GDPR, did not mention discrimination at all. However, neither do explicit references to intersectional discrimination appear in the GDPR. For example, Recital 71 GDPR considers discrimination with regard to a possible risk for the rights and freedoms of data subjects arising from profiling[49] based on racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation. The wording implies that these factors are to be considered separately rather than cumulatively and overlooks how other grounds (e.g., gender, age) could

[44] Gellert and others (n 6).
[45] Ivanova (n 15).
[46] Zuiderveen Borgesius (n 15).
[47] Ivanova (n 15); Naudts (n 15); Jenni Hakkarainen, 'Naming Something Collective Does Not Make It so: Algorithmic Discrimination and Access to Justice' (2021) 10 Internet Policy Review.
[48] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31–50.
[49] *Ex* Article 4(4) GDPR 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.

affect discrimination dynamics. Similarly, Recital 38 Law Enforcement Directive (LED),[50] sets data processing rules in the law enforcement sector. Likewise, Recital 75 GDPR and Recital 51 LED concerning risks arising from processing activities in general, and Recital 85 GDPR and Recital 61 LED describing possible damages deriving from data breaches, hint at discrimination, not all data breaches affecting people the same way. Even the explanatory memorandum to the AIR stresses the importance of including therein:

> '[…] specific requirements that aim to minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems' lifecycle […].'

Accordingly, Article 10 AIR sets certain quality criteria for training, validation and testing datasets to prevent bias. In the initial EU Commission proposal, the risks of discriminatory outcomes are among the reasons that led to the prohibition of social scoring (Recital 17 AIR) and to the classification of certain systems – biometric identification (Recital 33 AIR), AI systems used in education or vocational training (Recital 35 AIR), employment (Recital 36 AIR), credit scoring (Recital 37 AIR), for certain law enforcement activities (Recital 38 AIR) and migration, asylum and border control (Recital 39 AIR) – as high-risk (Recital 28 AIR). Plus, the technical documentation referred to in Article 11(1) AIR needs to include detailed information about the monitoring, functioning and control of the AI systems (Annex 4 Point 3 AIR) to address, *inter alia*, discrimination. Yet, again, intersectional discrimination does not appear.

Conversely, other legislation covering data-related matters seems to ignore not just intersectional discrimination-specific challenges, but that discrimination risks and bias may arise from data processing. For instance, in the Open Data Directive,[51] the Data Act Proposal[52] and the Data Governance Act,[53] having different scopes but overall aimed to favour data-sharing and the re-use of both public and, in some cases, private-sector information, discrimination is not addressed in the same terms as in the GDPR, the LED and the AIR. Despite public sector information being expected to

[50] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, p. 89–131.
[51] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). OJ L 172, 26.6.2019, p. 56–83.
[52] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM/2022/68 final.
[53] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). OJ L 152, 3.6.2022, p. 1–44.

be used to train AI systems, there are no safeguards as to how to ensure that this information is checked against possible bias. Non-discrimination matters are indeed exclusively dealt with in terms of entities that access information. Sharing information is the priority, regardless of the quality, bias-wise, thereof. Some may argue that this matter would be better addressed in the AIR and that the protection ensured by other data protection laws is sufficient. Nevertheless, including requirements to address bias, even in data-sharing-focused instruments, would provide extra safeguards to people and promote consistency of the legal framework. The fact that data are allegedly non-personal (e.g., because they refer to environmental or traffic information) does not mean they are bias-free. Conversely, sharing data without providing information as to the context of collection may lead to misinterpretations. More data does not necessarily entail more accurate data, as they may suggest misleading correlations.[54] Furthermore, considering that automated decision systems have a wider scope of applications than humans', algorithmic discrimination may expand at a quicker pace than merely human discrimination.[55]

Building upon this brief overview of how certain EU data protection law instruments deal with discrimination, it is possible to argue that, formally speaking, they do not represent a game-changer for intersectionality. They do not exclude that discrimination may be intersectional, but they do not expressly acknowledge it. Thus, to evaluate whether, in the substance, data protection law could be used to tackle intersectional discrimination issues, it is necessary to look into specific GDPR (and other data protection law) provisions. The next section offers a comparison between protected grounds and special categories of data.

### 3.2 Comparing Protected Grounds and Special Categories of Data

#### 3.2.1 The Average Individual under EU Anti-Discrimination and Data Protection Law

To a certain extent, the protected grounds under EU anti-discrimination secondary law – namely, sex (and to a limited extent, gender identity, in so far as a person is willing to or having undergone a gender reassignment surgery), racial or ethnic origins, age, disability, religion or belief and sexual orientation, nationality – overlap with the special categories of personal data under EU data protection law. Certain categories of personal data are considered more special than others because their misuse could lead to human rights abuses and/or individual harm.[56] Thus, this approach is similar to that used to identify protected grounds in anti-discrimination law. These data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of

[54] Janneke Evers, 'In de Schaduw van de Rechtsstaat: Profilering En Nudging Door de Overheid' (2016) 84 Computerrecht 167.
[55] Gerards and Xenidis (n 2).
[56] Ludmila Georgieva and Christopher Kuner, 'Article 9. Processing of Special Categories of Data', *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a natural person's sex life or sexual orientation, as listed in Article 9 GDPR. Other information is granted somehow a special treatment, although not formally labelled as special categories of personal data. For instance, Article 10 GDPR imposes restrictions on the processing of data related to criminal convictions and offences. Special rules on consent to data processing apply when children are involved (Article 8 GDPR), considering that 'they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data' (Recital 38 GDPR). Accordingly, the holder of parental responsibility needs to consent to the processing for those below 16 years old, or 13, depending on national laws specifying the GDPR. Whereas the GDPR does not consider financial information or location data, formally speaking, special categories, data protection regulators had recommended treating them carefully as they constitute data of a *highly personal nature*.[57] Thus, despite Article 9 GDPR being closed, the categories of information that can be considered sensitive are broader.

At the same time, important differences between the protected grounds under EU anti-discrimination secondary law and the special categories of data remain, particularly concerning the discipline of sex and gender identity,[58] age, disability and nationality. Sex and gender identity, indeed, are not considered sensitive information in data protection law, even if certain data protection regulators have emphasised how they can affect the vulnerability of data subjects, especially as to the effects of the processing.[59] Cases of women (of different races, ages and backgrounds) being discriminated against by automated tools used to support the screening of CVs and university admissions have been reported.[60] Likewise, it was noted how search engines could exacerbate stereotyping and objectifying of intersectionally situated groups (with racialised women more often associated with pornography than white women).[61] Furthermore, the predominant understanding of sex and gender in the overall law of the EU, and consequently in EU data protection law, still relies on the male/female binary, neglecting how, to better reflect human diversity, gender should

[57] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679'.

[58] 'Sex' entails the set biological and physiological characteristics that usually define humans as female or male, but may co-exist in the same person. 'Gender identity' refers to the 'internal and individual experience of gender, which may or may not correspond to the sex assigned at birth, including the personal sense of the body […] and other expressions of gender, including dress, speech and mannerisms'. European Institute for Gender Equality (EIGE), 'Glossary & Thesaurus'.

[59] Gianclaudio Malgieri and Gloria González Fuster, 'The Vulnerable Data Subject: A Gendered Data Subject?' (2022) 13 European Journal of Law and Technology.

[60] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016); Caroline Criado Pérez, *Invisible Women: Exposing Data Bias in a World Designed for Men* (Chatto & Windus 2019).

[61] Xenidis (n 30).

rather be understood as fluid and multidimensional.[62] Accordingly, certain technologies such as automated gender recognition have been deeply criticised for excluding transgender people.[63] In data protection law, only the young age of data subjects counts. No specific safeguards are foreseen for elderly persons, potential victims of the digital divide, nor for adults with mental disabilities, who could instead be considered in comparable situations with children. For these people, the empowerment measures under the GDPR (e.g., data subjects' rights, right to information) may be of very little use. Then, whereas information concerning disability may be encompassed in health and genetic data, the GDPR does not consider, for instance, how disability could impact the empowerment of the data subjects (in terms of e.g., accessibility of privacy notices, or exercise of data subjects' rights). Finally, nationality in data protection is not regarded *per se* as sensitive information, but only so far as it relates to race and ethnic origins.

These shortcomings led some academics to reflect upon the nature of the data subject under the GDPR. They concluded that, like the *average subject* in other areas of law, such as anti-discrimination, the data subject, namely the rational and free-willed individual supposed to exercise the rights thereof, is inherently white, male, able-bodied, heterosexual, cis-gender and educated.[64] They are also, possibly, documented, in so far as a controller may, albeit in exceptional cases, request an ID card to prove the identity of a data subject to enable the exercise of their rights.[65] Therefore, even in this sense, the GDPR does not innovate compared to other pieces of legislation that build upon a liberal understanding of fundamental rights.[66] Although more intersectional interpretations of the notion of data subjects seem possible and have been proposed,[67] they are not embedded in the structure of the Regulation.

### 3.2.2 Circumventing the Limitations of Article 9 GDPR and Anti-Discrimination Secondary Law through the Risk-Based Approach

Despite the list in Article 9 GDPR being closed, like the list of protected grounds in Article 10 TFEU, the definition of 'sensitive data' is potentially extremely broad

[62] Tetyana Krupiy, 'Why the Proposed Artificial Intelligence Regulation Does Not Deliver on the Promise to Protect Individuals from Harm' (*European Law Blog*, 2021).
[63] Foad Hamidi, Morgan Klaus Scheuerman and Stacy M Branham, 'Gender Recognition or Gender Reductionism? The Socialimplications of Automatic Gender Recognition Systems' (2018) 2018-April Conference on Human Factors in Computing Systems – Proceedings 1; Os Keyes, 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition' (2018) 2 Proceedings of the ACM on Human-Computer Interaction.
[64] Jens T Theilen and others, 'Feminist Data Protection: An Introduction' (2021) 10 Internet Policy Review 2; Malgieri and González Fuster (n 59); Aisha PL Kadiri, 'Data and Afrofuturism: An Emancipated Subject?' (2021) 10 Internet Policy Review.
[65] European Data Protection Board, 'Guidelines 01/2022 on Data Subject Rights– Right of Access' (2022).
[66] Theilen and others (n 64); Malgieri and González Fuster (n 59); Kadiri (n 64).
[67] Kadiri (n 64).

considering that, depending on the context, it is possible to make inferences about racial or ethnic origins, health status, etc. from seemingly neutral information, such as surnames or photos, or by combining different datasets[68] or by proxies like postal codes or dietary requirements.[69] In EU anti-discrimination law, discrimination based on proxies relating to protected grounds is forbidden in so far as it falls within the notion of indirect discrimination.[70] Instead, regardless of the broad formulation of Article 9 GDPR, proxies for sensitive data are not currently expressly granted special protection under EU data protection law. For example, it was noted how the GDPR does not provide safeguards for affinity profiling, namely a type of profiling that does not directly infer a user's sensitive data but builds upon other information to measure the user's affinity for certain groups, whose protection not only under EU data protection law but also under EU anti-discrimination law is questionable.[71] Furthermore, despite the protection of *inferred* sensitive information being recommended by the EU data protection regulators and hinted at by the wording of the GDPR, the scope thereof is uncertain.[72] For some authors, it is necessary to look at whether the controller intends to infer sensitive information. Others argue that if sensitive information is collected coincidentally it should not be treated as sensitive.[73] Others call for combining a purpose-based and contextual-based interpretation of the notion of sensitive data, arguing that:

> '[…] personal data should be considered sensitive IF the intention of the data controller is to process or discover sensitive information OR if it is reasonably foreseeable that, in a given context, the data in question can be used to reveal or to infer sensitive aspects of data subjects […].'[74]

In any event, this uncertainty is problematic considering the rise of proxy-discrimination performed by automated systems.[75] Admittedly, in the case C-184/20 *Vyriausioji tarnybinės etikos komisija*, the CJEU clarified at [120] that 'data that are capable of revealing the sexual orientation [*or any other sensitive information*] of a natural person by means of an intellectual operation involving comparison or deduction fall within the special categories of personal data […]' and that, to avoid compromising the effectiveness thereof, the processing of personal data liable indirectly to reveal sensitive information concerning a natural person cannot be excluded from the strengthened protection regime. Thus, the CJEU seems to admit a broad understanding of the notion of special categories of data. However, the

[68] Paul Quinn, 'The Difficulty of Defining Sensitive Data-The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22 German Law Journal 1583.
[69] Georgieva and Kuner (n 56).
[70] Gellert and others (n 6).
[71] Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35 Berkeley Technology Law Journal 2.
[72] ibid.
[73] ibid.
[74] Quinn (n 68).
[75] Anya ER Prince and Daniel Schwarcz, 'Proxy Discrimination in the Age of Artificial Intelligence and Big Data' (2020) 105 Iowa Law Review 1257.

judgment does not specify how far such analysis on the suitability of data to reveal sensitive information needs to go, nor does it recognise a role to the intention of the controller, meaning that many issues remain open. Furthermore, considering that automated systems may even identify newly invented classes or irrelevant correlations in data, discrimination may occur based on information that is not even a proxy for sensitive attributes, thus remaining outside both the scope of data protection and anti-discrimination law.[76] For instance, a Dutch insurance company was found to charge more customers living in apartments whose civic number contains a letter.[77]

What is certain is that neither data protection nor anti-discrimination secondary laws provide enough flexibility to introduce new special categories of data or protected grounds that would instead deserve protection when adopting an intersectional approach. For example, despite *property* being mentioned in Article 21 CFR, social status (or class) is not protected under the EU secondary law anti-discrimination legal framework. Financial information, from which it is possible to infer social status, is not expressly protected in data protection law either. Depending on the context, apparently neutral information such as whether a person lives in a rural or urban area may be relevant under the intersectionality principle.[78]

However, to a certain extent, the GDPR allows circumventing the limited scope of the letter of Article 9 GDPR and, consequently, the limited scope of the protected grounds in EU anti-discrimination secondary law. Indeed, the GDPR builds upon a risk-based approach, such that different compliance measures are triggered depending on the riskiness of the processing operations, determined *inter alia* by the nature of the data. In the GDPR, traditional right-based constructs (e.g., data processing principles and data subjects' rights) are combined with other tools (e.g., DPIAs, data security, data protection by design) pertaining to the domain of risk analysis, i.e., the activity of assessing and managing risks.[79] For instance, when the risks deriving from the data processing are high, controllers must carry out a DPIA or adopt different technical and organisational measures. Potentially, due to the openness of the notion of risk, and depending on the context, any information whose processing affects the rights and freedoms of data subjects, and thus that can determine discrimination, could be treated as sensitive.[80] For instance, while a company planning to implement an

[76] Zuiderveen Borgesius (n 15).
[77] Janneke Gerards and Frederik Zuiderveen Borgesius, 'Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence' (2022) 20 Colorado Technology Law Journal 1.
[78] Kathy Davis, 'Intersectionality as a Critical Mathodology' in Nina Lykke (ed), *Writing Academic Texts Differently: Intersectional Feminist Methodologies and the Playful Art of Writing* (Routledge 2014).
[79] Raphaël Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2 European Data Protection Law Review 481.
[80] Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' (2020) 37 Computer Law and Security Review; Malgieri and González Fuster (n 59).

automated screening for CVs may be aware of how these systems are prone to discriminate based on e.g., gender and/or social status (for instance, privileging male candidates coming from expensive universities), through a DPIA process, it could be possible identify and address the risks arising from the processing of this information, or proxies thereof, despite not being formally qualified as special categories.

This interpretation is confirmed by the opinions and guidance issued by data protection regulators, which despite not being legally binding maintain authoritative value, especially for practitioners. As mentioned above, for instance, whereas the GDPR does not consider financial information or location data, formally speaking, as a special category, data protection regulators have recommended treating them carefully.[81] The importance of DPIAs in relation to automated systems is supposed to grow in the future in so far as they are also mentioned by Article 29 AIR, which states that:

> 'Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.'

The flexibility granted by the risk-based approach could be extremely beneficial to addressing cases of intersectional discrimination, allowing coverage of grounds otherwise neglected in both EU data protection and anti-discrimination legislative frameworks and freely combine them. Nevertheless, it has major shortcomings. First, it might be argued that broadly interpreting the notion of special categories of data would go against the letter of the GDPR, which opted for a closed list thereof. However, as witnessed in C-184/20 *Vyriausioji tarnybinės etikos komisija* the CJEU appears to consider legitimate such a wide interpretation. Secondly, the evaluation of the risk, and also of the sensitivity of the information processed depending on the circumstances, is left to the discretion of data controllers.[82] Such subjectivity of the evaluation of the suitability of data to reveal sensitive information is not resolved by the judgment *Vyriausioji tarnybinės etikos komisija*. Even the possibility of scrutiny of DPAs on the decisions of data controllers in terms of risk evaluation are limited. DPAs may have a say on such evaluations only within the framework of an enforcement action or if they are requested to give advice by a controller who triggers the prior consultation mechanism *ex* Article 36 GDPR.

### 3.3 Rules Applicable to Sensitive Data

The GDPR forbids the processing of special categories of data unless one of the (admittedly many) exceptions foreseen in Article 9(2) GDPR applies. Similarly, the LED

[81] Article 29 Data Protection Working Party (n 57).
[82] Reuben Binns, 'Data Protection Impact Assessments : A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22.

allows the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation only when strictly necessary, subject to appropriate safeguards for rights and freedoms only at certain conditions (Article 10 LED). Thus, the EU data protection legal framework acknowledges the importance of special categories of data (and consequently certain protected grounds under anti-discrimination law, in so far as they overlap) by granting them stronger legal protection. The structure of the GDPR and the LED seems to suggest that it is more privacy-friendly to avoid processing this type of information, and thus that the rule is not to process sensitive data unless certain conditions apply.[83] This approach also seems to be confirmed by Article 22 GDPR, perhaps one of the most relevant in terms of automated decision-making and bias.[84] Setting aside the broader debate on the scope thereof,[85] under Article 22 GDPR, data subjects have the right not to be subject to a decision producing legal or similarly significant effects on them when based solely on automated decision-making, including profiling (unless such decision is necessary for the performance of a contract, is authorised by Union or Member States law, or is based on data subjects' explicit consent). Article 22 GDPR forbids basing such automated decisions on special categories of data, as the use of this information is allowed only when the conditions set in Article 9(2)(g) GDPR apply[86] or when the data subject has given explicit consent *ex* Article 9(2)(a) GDPR.

[83] Note however that not all EU data protection law builds upon this principle. For instance, the processing of biometric data is a core function in EU large-scale databases. Simone Casiraghi and Alessandra Calvi, 'Biometric Data in the EU (Reformed) Data Protection Framework and Border Management' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI-Global 2020).

[84] Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (2020).

[85] Some commentators, certain courts and the European Data Protection Board argue that Article 22 GDPR entails a ban for controllers to take decisions having legal or other significant effects on data subjects based solely on automated decision-making. Yet, others argue that the letter of Article 22 does not forbid such decision-making, but only establishes a right for individuals not to be subject to it. Accordingly, controllers could still rely on solely automated systems to take decisions significantly affecting data subjects in so far as they grant them the rights to object the processing and obtain human intervention. Isak Mendoza and Lee A Bygrave (2017), 'The Right Not to Be Subject to Automated Decisions Based on Profiling' [2017] EU Internet Law: Regulation and Enforcement 77; Lee A Bygrave, 'Article 22. Automated Individual Decision-Making, Including Profiling', *The EU General Data Protection Regulation: A Commentary – Update of Selected Articles* (Oxford University Press 2021). Luca Tosoni, 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' (2021) 11 International Data Privacy Law 145; Lee A Bygrave, 'Article 22. Automated Individual Decision-Making, Including Profiling', *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[86] Namely, the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Yet, framing the processing of sensitive data as something always exceptional, especially when automated systems are employed, may be misleading. Whereas *prima facie* avoiding processing sensitive information may seem a solution to protect individuals, in reality, this approach legitimises the existence of data gaps and hinders bias detection, monitoring and correction.[87] Knowledge of protected characteristics is both necessary and problematic to prevent and address (intersectional) discrimination.[88] For instance, from a computing perspective, collecting sensitive categories of data is necessary when automated decision-making systems are trained to prevent bias. At the same time, processing special categories of data may be necessary to allow public and private entities to draw statistics on diversity (e.g., at the workplace) and even evaluate the effectiveness of the positive actions (if any) undertaken to promote substantial equality.[89] Thus, depending on the context, processing such types of information should be considered the rule to avoid fundamental rights violations. That is why data protection law, rather than preventing sensitive data collection, should instead create a framework for ensuring their use, at the same time granting them adequate and reinforced protection.[90] Accordingly, the GDPR foresees certain extra obligations for controllers when they process special categories of data on a large scale, like appointing a data protection officer or performing a DPIA.[91] However, this approach has advantages and drawbacks.

On the one hand, even when data controllers are committed to collecting sensitive information from data subjects to prevent, monitor and correct bias, and therefore, discrimination, data subjects may still refrain from voluntarily sharing this information with them. Either because they are not duly informed about the importance of sharing this type of information to combat discrimination, but especially considering that, despite any good intentions, controllers remain in the position of using sensitive information to discriminate against them.[92] After all, special categories of data have been used in the past to perpetrate human rights violations, and it is only recently that their processing has been deemed necessary to conversely prevent harm. Due to this understandable lack of trust, data subjects may refuse to share sensitive information with controllers, even against their immediate interests. Major concerns depend on the fact that people may be uneasy at having their sensitive data stored, regardless of any restrictive access policy thereof; the possibility of such data being re-used and repurposed, either due to data breaches or to changes in policies that could lead to over-surveillance of certain categories of people (see e.g., the debate on the interoperability of EU large-scale databases, blurring the lines between

[87] Criado Pérez (n 60).
[88] Michael Veale and Reuben Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data' (2017) 4 Big Data and Society 1.
[89] Laraine Laudati, 'Summaries of EU Court Decisions Relating to Data Protection 2000-2015' 59).
[90] Indrė Žliobaitė and Bart Custers, 'Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models' (2016) 24 Artificial Intelligence and Law 183.
[91] Quinn (n 68).
[92] Veale and Binns (n 88).

immigration and law enforcement[93]); and the possible misuses perpetrated by data collectors if the exception to collect sensitive information is interpreted too broadly.[94]

To address these issues to at least some extent, some authors suggest that the processing of sensitive information should be performed by trusted third parties instead of controllers. This way, sensitive information would still be processed and could be used to prevent bias and discrimination, but not by the entities that could use them to the detriment of the data subjects.[95] A similar solution has been adopted in the Netherlands, where companies with more than 250 employees may ask the Central Bureau of Statistics to measure the diversity of their personnel by combining the non-sensitive data held by them with the sensitive information held by the bureau.[96] Unfortunately, this practice is not widespread.

The issue as to the nature of such trusted third parties also remains open. Indeed, governmental entities may not be perceived as sufficiently trustworthy by all sectors of the population, especially by those historically oppressed. That is why NGOs might be more suited to play this role, provided that they are entrusted with enough resources, as well as in terms of cybersecurity. Other authors propose relying on independent supervisory authorities for this.[97] Another possibility, the technical feasibility of which is uncertain considering possible losses in the utility of data, would be to build synthetic datasets keeping an equivalent distribution of individuals across protected groups based on the real ones, whose storage could be thus limited.[98]

In any event, the above demonstrates that the *explicit consent* exception to the processing of special categories of data *ex* Article 9(2)(a) GDPR does not constitute an effective legal basis as it creates a sort of short-circuit by rightfully empowering data subjects to avoid having their sensitive data processed whilst practically raising obstacles to bias and discrimination prevention, monitoring and correction performed by *bona fide* controllers. Other than the attitude of data subjects towards their sensitive information, limitations of the explicit consent legal basis depend on the consent requirements, too. Even when data subjects agree to share their sensitive information, the existence of an imbalance between them and controllers (e.g., in work relationships) could undermine their consent, considering that, to be valid, consent needs to be freely given (other than specific, unambiguous and informed).[99]

---

[93] Alessandra Calvi, 'Border Management Law in the European Union' in J. Peter Burgess and Dariusz Kloza (eds), *Border Control and New Technologies* (ASP 2021).
[94] Marvin Van Bekkum and Frederik Zuiderveen Borgesius, 'Using Sensitive Data to Prevent Discrimination by Artificial Intelligece: Does the GDPR Need a New Exception?' (2022) 48 Computer Law & Security Review 105770 <https://doi.org/10.1016/j.clsr.2022.105770>.
[95] Veale and Binns (n 88).
[96] Konstantinos Bartzeliotis, 'Overview of the Grounds and Fields in Which Positive Action Is Being Implemented' in 'Exploring Positive Action as a Means to Fight Structural Discrimination in Europe' (2021).
[97] Bekkum and Borgesius (n 94).
[98] ibid.
[99] ibid.

On the other hand, from a legal compliance point of view, it may be easier for controllers not to process sensitive data at all, in order to avoid incurring extra data protection compliance measures, even if this entails a greater risk of bias.[100] Therefore, data controllers may purposedly refrain from processing sensitive information, unless they are legally obliged to do so. Many of the exceptions in Article 9(2) GDPR build upon the existence of a legal obligation on data controllers justifying the processing of special categories of data. Thus, said exceptions would allow data controllers to circumvent the need to acquire explicit consent from data subjects. However, such an approach could also be problematic, considering that mandating the disclosure of sensitive information could undermine data subjects' autonomy, especially in where the entities who process sensitive data coincide with those that remain in the position of discriminating.

Some of the law-based exceptions are related to domains protected under EU anti-discrimination secondary law. For instance, processing sensitive data in the field of employment and social security (Article 9(2)(b) GDPR) or for the assessment of the working capacity of an employee or management of social care systems (Article 9(2)(h) GDPR). Even the exception *ex* Article 9(2)(j) GDPR, which legitimises the collection of special categories of data for statistical purposes, could be invoked by a controller for the collection of equality data. However, for the exceptions to be applicable, the processing of special categories of data needs to be necessary for statistical purposes,

> 'based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject'.

Currently, equality data legislation across the EU is rather scarce and scattered, and does not always cover a wide variety of protected grounds.[101]

In any event, in light of the insufficient elaboration of intersectional discrimination under EU anti-discrimination secondary law, as well as the difficulties of reflecting intersectional discrimination in a quantitative way (due to the structural limitations of the additive approach towards collecting information on protected grounds, that may reflect multiple but nor intersectional discrimination[102]) looking at all these exceptions may be of little use to evaluate whether they could be used to tackle

[100] Quinn (n 68).
[101] Timo Makkonen, *European Handbook on Equality Data – 2016 Revision* (Publications Office of the European Union 2016); Lara Ferguson Vázquez de Parga and Imane El-Morabet, 'Debates about Positive Action Measures and Their Effectiveness' in 'Exploring Positive Action as a Means to Fight Structural Discrimination in Europe' (2021).
[102] Lisa Bowleg, 'When Black + Lesbian + Woman ≠ Black Lesbian Woman: The Methodological Challenges of Qualitative and Quantitative Intersectionality Research' (2008) 59 Sex Roles 312.

intersectional discrimination. Instead, a more valid alternative to overcome these limitations is to look at the exception of substantial public interest *ex* Article 9(2)(g) GDPR.

### 3.4 The Exception *ex* Article 9(2)(g) GDPR: A Substantial Public Interest to Address Intersectional Discrimination?

Pursuant to Article 9(2)(g) GDPR, processing of special categories of personal data is allowed when necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Thus, contrary to private interest processing, where it is the controller who balances interests, in public interest processing, the (EU or Member State) legislator identifies the public interests and balances them against the rights of individuals.[103] The threshold to satisfy a substantial public interest is very high, much more than the reference to the public interest in Article 6(1)(e) GDPR. Recital 46 GDPR refers, for instance, to humanitarian purposes or the operation of democratic systems.[104] However, there are no other examples of substantial public interests in the Regulation. Even data protection regulators' guidance on the *substantial public interest* exception is rather scarce and scattered. At a national level, the Belgian DPA has singled out certain situations where Article 9(2)(g) GDPR applies.[105] Likewise, the Information Commissioner Office (i.e., the UK's DPA) has identified certain substantial public interest conditions, that include, for instance, 'Equality of opportunity or treatment' and 'Racial and ethnic diversity at senior levels'. The European Data Protection Board dealt with Article 9(2)(g) GDPR only marginally, especially during the COVID-19 pandemic, and without considering how the substantial public interest could be interpreted in relation to intersectional discrimination.[106] However, para 55 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and

[103] Athena Christofi, Ellen Wauters and Peggy Valcke, 'Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?' (2021) 12 European Journal of Law and Technology.

[104] Georgieva and Kuner (n 56).

[105] Like 'processing by associations with a legal personality or foundations, whose main statutory objective is to defend and promote human rights and fundamental freedoms, and processed in order to achieve that objective, provided that the processing has been authorised by the King by a decree adopted after consultation in the Federal Council of Ministers, after advice from the competent supervisory authority.' Or 'processing managed by the Center for Missing and Sexually Exploited Children for the receipt, transmission to the judicial authorities and follow-up of data concerning persons suspected of having committed a crime or malpractice in a particular case of missing or sexually exploited children.' <https://www.dataguidance.com/notes/belgium-data-protection-overview> (accessed on 12/10/2023).

[106] See e.g., the 'EDPB Statement on the processing of personal data in the context of the COVID-19 outbreak', adopted on 19 March 2020; the 'EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research', adopted on 2 February 2021.

the GDPR could provide some help on the interpretation of Article 9(2)(g) GDPR. There, the EDPB stated that:

> '[…] the processing of the special categories of personal data has to be addressed in a specific derogation to Article 9(1) GDPR in Union or Member State law. This provision will have to address the proportionality in relation to the pursued aim of the processing and contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Furthermore, this provision under Union or Member State law will have to respect the essence of the right to data protection. Finally, the processing of the special categories of data must also be demonstrated to be necessary for the reason of the substantial public interest, including interests of systemic importance. Only when all of these conditions are fully met, this derogation could be made applicable […].'

Can addressing intersectional discrimination be considered a reason of substantial public interest? Does EU (or Member State) law foresee a specific derogation to Article 9(1) GDPR? If so, does this provision address proportionality in relation to the pursued aims and include specific safeguards for data subjects? Does this provision respect the essence of the right to data protection? Is processing sensitive categories of data necessary to prevent intersectional discrimination?

Arguably, the fight against discrimination can be considered a reason of substantial public interest.[107] After all, a general principle of equality permeates the European legal framework and the EU evolved as a key player in the protection of fundamental rights.[108] Article 2 TFEU states that:

> 'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.'

Furthermore, the list of protected grounds under Article 21 CFR is flexible and open-ended. Thus, regardless of the difficulties in the conceptualisation thereof, it seems reasonable to state that the fight against intersectional discrimination represents a substantial public interest in the EU legal order. However, this is not sufficient. The conditions previously identified need to exist cumulatively. It is necessary to identify, in EU or Member State law, a specific derogation for data processing, which at the same time addresses proportionality in relation to the pursued aims and includes specific safeguards for data subjects. That respects the essence of the right to data protection. And that the processing of special categories of data is necessary to address intersectional discrimination. It has been seen how the scope of EU anti-discrimination secondary law remains scattered, sectorial and unable to cover cases

[107] Ivanova (n 15).
[108] Gellert and others (n 6).

of intersectional discrimination.[109] Thus, that field of law appears of little use when looking for a legal basis to ground the processing of sensitive data. An alternative solution is to look at the AIR, whose scope of application, despite the broadness of the definition of AI, remains nevertheless limited to automated systems.[110] Article 10(5) AIR acknowledges that:

> 'To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.'[111]

*Prima facie*, Article 10(5) AIR seems to comply with the requirements set by Article 9(2)(g) GDPR as specified by the EDPB. By acknowledging the insufficiency of approaches to fairness through unawareness of protected characteristics,[112] it sets a specific derogation to Article 9 (and corresponding articles in other EU data protection laws). It addresses proportionality *latu sensu* in so far as it sets a (strict) necessity condition of sensitive data processing for the specific purposes of bias monitoring, detection and correction in relation to high-risk AI systems. Despite not being a specific provision on intersectional discrimination, it may be nevertheless functional to address it. Whether this provision respects the essence of the right to data

[109] ibid.

[110] Bekkum and Borgesius (n 94).

[111] The European Parliament proposed to further specify the provision in the DRAFT Compromise Amendments of 9th May 2023, adding that '[…] In particular, all the following conditions shall apply in order for this processing to occur: (a) the bias detection and correction cannot be effectively fulfilled by processing synthetic or anonymised data; (b) the data are pseudonymised; (c) the provider takes appropriate technical and organisational measures to ensure that the data processed for the purpose of this paragraph are secured, protected, subject to suitable safeguards and only authorised persons have access to those data with appropriate confidentiality obligations; (d) the data processed for the purpose of this paragraph are not to be transmitted, transferred or otherwise accessed by other parties; (e) the data processed for the purpose of this paragraph are protected by means of appropriate technical and organisational measures and deleted once the bias has been corrected or the personal data has reached the end of its retention period; (f) effective and appropriate measures are in place to ensure availability, security and resilience of processing systems and services against technical or physical incidents; (g) effective and appropriate measures are in place to ensure physical security of locations where the data are stored and processed, internal IT and IT security governance and management, certification of processes and products; Providers having recourse to this provision shall draw up documentation explaining why the processing of special categories of personal data was necessary to detect and correct biases.'

[112] Calvi and Kotzinos (n 37).

protection is uncertain, since the meaning of 'essence' is a topic of much debate.[113] Admittedly, Article 10(5) AIR creates an important interference in the right to personal data protection, as the processing of sensitive data is an extremely intrusive practice. Yet, the object of protection of data protection law is not data *per se* but the persons to whom the information refers.[114] Whereas from the processing of sensitive information it is possible to achieve greater protection of the people to whom the information refers, this does not appear to be blatantly in contrast with the essence of the right to data protection.

Instead, what could be problematic in terms of respect of the essence is the lack of measures equivalent to data subjects' rights in the AIR. Whereas people are denied the right to oppose such processing of sensitive information, this may be in contrast with the idea of essence.[115] However, considering that in the case of the exception *ex* Article 9(2)(g) it is the legislator (EU or Member State) that is supposed to identify the public interests and balance them against the rights of individuals,[116] it is also reasonable to conclude that the controller will not have to determine whether the provision complies with the essence of data protection right, being the compliance of secondary law, in this case the AIR (if ever adopted), with the CFR presumed.[117]

As regards the necessity of processing sensitive data for bias monitoring, detection and correction, scholars are quite consistent in defending it.[118] Even further, as noted above, Article 10 AIR refers to strict necessity, not just to necessity. It is true that due to the intrusiveness of the practice of processing sensitive data, some authors suggest alternative paths to sensitive data collection to mitigate discrimination, such as reliance on collaborative online platforms allowing experience-sharing on unsupervised learning.[119] However, these techniques are new and still underexplored,

---

[113] Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864; Dara Hallinan, 'The Essence of the Right to the Protection of Personal Data: Essence as a Normative Pivot' (2021) 12 European Journal of Law and Technology; Lorenzo Dalla Corte, 'A Right to a Rule: On the substance and essence of the fundamental right to personal data protection' in Dara Hallinan and others (eds), *Data protection and privacy: Data protection and democracy* (Hart Publishing 2020).

[114] Mireille Hildebrandt, '"Practical and Effective Protection" of Human Rights in the Era of Data-Driven Tech: Understanding European Constitutional Law' <https://cyber.jotwell.com/practical-and-effective-protection-of-human-rights-in-the-era-of-data-driven-tech-understanding-european-constitutional-law/> (accessed on 12/10/2023); Marion Albers, 'Realizing the Complexity of Data Protection' in Serge Gutwith and others (eds), *Reloading Data Protection* (Springer Netherlands 2014) <http://link.springer.com/10.1007/978-94-007-7540-4_11> (accessed on 12/10/2023).

[115] Brkan (n 113).

[116] Christofi, Wauters and Valcke (n 103).

[117] Dariusz Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process' [2020] d.pia.lab Policy Brief, VUB 1.

[118] Žliobaitė and Custers (n 90).

[119] Veale and Binns (n 88).

meaning that, at least for the moment, the *necessity condition* still appears fulfilled. Finally, the Article sets some (admittedly generic) safeguards for data subjects, such as the implementation of privacy-preserving and data security measures.[120] Thus, if and when the AIR is approved, it could provide an EU legal basis for legitimising the processing of sensitive data to ensure bias monitoring, detection and correction, at least when high-risk AI systems are involved.

Regardless of the letter of Article 10(5) AIR, some technical constraints remain. Consider that (group) fairness metrics seem essential to comply with many requirements of the AIR, including Article 10 AIR.[121] Even if intersectional approaches to technical fairness are increasingly under scrutiny, current metrics are not suitable to properly address intersectionality concerns. So far, intersectionality has been operationalised by collapsing the membership to different subgroups into a unique attribute, an oversimplification against the rationale of this concept.[122] Then, fairness metrics enable comparison of only two groups at a time, making intersectional analysis extremely difficult.[123]

Then, other limitations lay in the wording of Article 10 AIR and the proposal considered overall. Whereas Article 9(2)(g) GDPR refers to data controllers, the obligation in Article 10(5) AIR is binding upon *providers*. The two notions will not necessarily coincide, as 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge (Article 3(3) AIR). Thus, whereas a controller does not coincide with a provider, it is uncertain whether the exception based upon Article 9(2)(g) GDPR read in conjunction with Article 10(5) AIR could be applicable.

Furthermore, Article 10(5) AIR does not set a clear legal obligation to use sensitive information in so far as *may* entails a possibility, rather than an obligation as with *shall*. Thus, controllers could invoke the exception if they are willing to process sensitive data, but the formulation of the article seems too flexible to entail a legal obligation. The justification of processing is framed in terms of *strict necessity* for bias monitoring, detection and correction, and not mere *necessity*, which is conversely the requirement of Article 9(2)(g) GDPR. Thus, providers seem even more restricted than controllers when processing special categories of data, even if their activity has been deemed essential to combat bias. What if the two notions of controller and provider coincide? Will necessity or strict necessity apply? Then, Article 10 AIR applies only to high-risk AI systems, whereas it may be desirable to perform bias checks in other

[120] Nevertheless, amendments proposed by the European Parliament were aimed at further specifying these safeguards.
[121] Calvi and Kotzinos (n 37).
[122] Agathe Balayn and Seda Gürses, 'Beyond Debiasing – Regulating AI and Its Inequalities' (2021).
[123] ibid.

situations carrying risk. Very importantly, the provision refers to Article 9 GDPR and corresponding articles in other laws. However, these articles do not exhaust the list of protected grounds that are conversely important to detect situations of intersectional discrimination.[124] Article 9 GDPR does not include, for example, information about sex and gender (and how are sex and gender being defined?), nor about social status, age, etc. This does not mean that this information cannot be processed for a bias check. However, the Article seems to wrongly hint that the grounds mentioned under Article 9 GDPR are sufficient.[125]

It was noted above how the entire AI debate and consequently the AIR, whilst insisting on the importance of tackling bias and unfairness in technologies, seem to neglect both how the complexity of human identities cannot be captured by mathematical formulas and that instead of focusing on the bias embedded in technologies, governments should rather tackle the structural inequalities still existing in many sectors where automated systems are deployed.[126] Otherwise, paradoxically, technically fair technologies will be deployed in an unfair and discriminatory context. Other lines of criticism denounce the excessive focus on debiasing datasets used to train models, whilst models themselves or outputs thereof may still be biased; and overlooking that fairness metrics have their own important limitations, risk oversimplifying complex problems of social justice and have been researched and – more or less successfully – applied only in a small set of social domains.[127] In particular, it was noted how current rules contained in the AIR give providers too much discretion in determining what counts as discrimination, when it occurs and how to address it, a problem exacerbated by the lack of sufficient independent auditing bodies.[128]

### 3.5 Enforcing Intersectional Discrimination Claims: The Role of Data Protection Law

Finally, to evaluate whether data protection law can be considered an enabler of intersectionality, it is necessary to look at the enforcement mechanisms thereof. As a general rule, for discrimination matters, to bring a case in court, a claimant needs to demonstrate that *prima facie* harm has occurred or is likely to occur and that such harm significantly and disproportionally affects (or is likely to affect) a protected group of people compared with others in a similar situation. Then, the claimant will

[124] Wachter (n 71).
[125] In that sense, the wording proposed in the Draft Opinion of the Committee for Legal Affairs of 2 March 2022 seem more appropriate: 'To the extent that it is strictly necessary […] the providers may ***also*** process […]'.
[126] Tetyana Krupiy, 'A Vulnerability Analysis: Theorising the Impact of Artificial Intelligence Decision-Making Processes on Individuals, Society and Human Diversity from a Social Justice Perspective' (2020) 38 Computer Law and Security Review 105429 <https://doi.org/10.1016/j.clsr.2020.105429>.
[127] Balayn and Gürses (n 122); Calvi and Kotzinos (n 37).
[128] Balayn and Gürses (n 122).

benefit from a reversal of the burden of proof.[129] However, these proceedings in the face of algorithmic discrimination seem insufficient. It was noted above that algorithmic discrimination may remain hidden from both victims and organisations and thus not enforceable under traditional instruments of anti-discrimination law (for example, when performed by algorithms that function as black boxes).[130] Furthermore, anti-discrimination law suffers from an enforcement gap for intersectional claims. The very same need to rely on the intermediation of a court could also be exclusive. Certain authors emphasise how, despite the existence, formally speaking, of a right to access to justice, substantially, such right is not exercised the same way by different categories of people.[131] Does data protection law allow for circumventing these gaps? In principle, it does, but with some caveats.

As regards the possible advantages, contrary to anti-discrimination law, the GDPR equips individuals with certain rights directly actionable against a data controller, without the intervention of a third party entrusted with a legal hermeneutics activity, i.e., a court.[132] For example, under Article 22 GDPR, data subjects have the right not to be subject to a decision producing legal or similarly significant effects on them when based solely on automated decision-making, including profiling (unless such decision is necessary for the performance of a contract, is authorised by Union or Member States law or is based on data subjects' explicit consent). Thus, where individuals believe that they have been discriminated against by an automated system, regardless of on which grounds, individually or intersectionally, they can object to the decision (Article 21 GDPR) and ask to have it revised by a human (Article 22(3) GDPR). Case law demonstrates how students and gig workers have already relied on Article 22 GDPR to complain about discrimination and how DPAs have engaged with investigations *ex officio* due to suspected cases of discrimination by automated systems (although, admittedly, the intersectional profile thereof has not been highlighted).[133]

Therefore, Article 22 GDPR could support the *ex post* detection of bias in automated systems. Yet, to effectively exercise the right, data subjects must be aware of the existence of automated decision-making and receive meaningful information about the logic involved, and about the significance and the envisaged consequences of the processing on them (Right to information *ex* Article 13(2)(f) and Article 14(2)(g), and Right to access *ex* Article 15(1)(h) GDPR), to understand how to correctly frame their

[129] Wachter, Mittelstadt and Russell (n 21); Gellert and others (n 6).
[130] Zuiderveen Borgesius (n 15); Hacker (n 15); Xenidis (n 31); Gerards and Xenidis (n 2).
[131] Bart van der Sloot and Sascha van Schendel, 'Procedural Law for the Data-Driven Society' (2021) 30 Information and Communications Technology Law 304 <https://doi.org/10.1080/13600834.2021.1876331>; Maroš Matiaško, 'Access to Justice through Lenses of Vulnerability and Equality: A Dialogue between Philosophy and Law' (2021) 22 ERA Forum 717 <http://dx.doi.org/10.1007/s12027-021-00696-0>.
[132] Gellert and others (n 6).
[133] Sebastião Barros Vale and Gabriela Zanfir-Fortuna, 'Automated Practical Cases from Courts Under the GDPR: Decision-Making and Data Protection Authorities' (2022).

claim.[134] Otherwise, the text of Article 22 GDPR would be a dead letter, or, as it has been argued, a 'second class data protection right'.[135] Similar restrictions to the use of automated individual decision-making, and the right to obtain human intervention, also exist in the law enforcement sector, but they are more limited in scope.

Regrettably, it is still extremely difficult for data subjects to understand whether their personal information is collected and by whom,[136] thus *a fortiori* to be aware of automated decision-making. Another point to consider is that data subjects may lack knowledge about their rights and be unaware that algorithms can discriminate against them. If they suspect they have been (intersectionally) discriminated against, data subjects would have to preliminarily exercise their right to information, connected to transparency, and access.[137] The effectiveness of the right to transparency has been subject to severe criticism as providing transparent information about the logic behind an automated decision may be impossible;[138] and the disclosure of certain information may be protected due to intellectual property considerations.[139] When information is eventually disclosed, it may be of little use unless a data subject has sufficient technical skills to interpret it, even if scholars recommend that the concept of meaningful information ought to be interpreted in light of the competences of data subjects.[140] Furthermore, when a decision is not based solely but just *largely* on automated decision-making, which is arguably the case in many algorithmic decisions, the applicability of the safeguards *ex* Article 22 GDPR is uncertain.[141] Although it was demonstrated that DPAs across the EU still managed to protect data subjects and identify GDPR infringements notwithstanding the inapplicability of Article 22 GDPR,[142] this remains nevertheless a limitation. Then, considering that the GDPR applies exclusively to personal data, predictive models and other forms of data analytics, unless applied to specific individuals, would remain outside the scope thereof.[143]

Whereas the direct enforcement against a data controller may represent an advantage compared with anti-discrimination law, this is not a silver bullet. First, recall that the personal characteristics of data subjects may affect the way they

[134] Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 International Journal of Law and Information Technology 91.
[135] Guillermo Lazcoz and Paul De Hert, 'Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems. Essential Pre-Requisites against Abdicating Responsibilities' (2022) 8 Brussels Privacy Hub Working Paper.
[136] van der Sloot and van Schendel (n 131).
[137] Hacker (n 15).
[138] Zuiderveen Borgesius (n 15); Gerards and Xenidis (n 2).
[139] Wachter, Mittelstadt and Russell (n 21).
[140] Bart Custers and Anne Sophie Heijne, 'The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice' (2022) 46 Computer Law and Security Review 105727 <https://doi.org/10.1016/j.clsr.2022.105727>.
[141] Zuiderveen Borgesius (n 15).
[142] Barros Vale and Zanfir-Fortuna (n 133).
[143] Zuiderveen Borgesius (n 15); van der Sloot and van Schendel (n 131).

exercise their rights.[144] Then, in case controllers do not follow up on their requests (and it was noted how EU data protection law suffers compliance and enforcement deficit[145]), data subjects will have to bring their claims in front of a DPA or a court. These procedures could be costly and time-consuming for data subjects.[146] Empirical studies on GDPR enforcement show how national practices for lodging a complaint across EU Member States remain inconsistent, even requiring different levels of supporting evidence for such claims, and how data subjects usually fail to receive information about the steps to take after lodging a complaint.[147] Considering the political character of intersectionality, DPAs and courts will not necessarily elaborate upon intersectional discrimination issues. Furthermore, many methods to tackle (intersectional) discrimination implicitly assume that controllers are party to sensitive information, whereas this is not necessarily the case.[148] Another major source of concern is that most legal regimes would still require a data subject to demonstrate individualisable harm, whilst automated decision-making could affect larger groups or clusters of the population. The possibility of complaining about (data) policies against the rule of law is much more limited,[149] and actions advocating for a public interest in data protection are currently not possible.[150] Likewise, the role of NGOs in GDPR enforcement remains largely overlooked.[151]

Another advantage of the GDPR is to effectively combine *ex post* data protection enforcement mechanisms (e.g., data subjects' rights) with *ex ante* tools, such as DPIAs.[152] Due to their anticipatory nature, these instruments would be suitable to prevent damages, including intersectional discrimination, and, consequently, the necessity to access *ex post* remedies, circumventing all the limitations arising therefrom.[153] However, again, their use is discretionary to data controllers. And the capacity of DPAs to ensure compliance of the controller with such data protection rules has been questioned, *inter alia* due to the limited resources that DPAs have to carry out investigations.[154] Consider also that due to recent legislative developments, DPIA is no longer the only type of assessment that can be relevant for automated systems. The AIR foresees a Conformity Assessment procedure, whilst the European Parliament has proposed to include therein a Fundamental Rights Impact Assessment.

---

[144] Malgieri and González Fuster (n 59).
[145] Zuiderveen Borgesius (n 15).
[146] van der Sloot and van Schendel (n 131).
[147] Gloria González Fuster and others, 'The Right to Lodge a Data Protection Complaint: OK, but Then What?' (2022).
[148] Zuiderveen Borgesius (n 15).
[149] van der Sloot and van Schendel (n 131).
[150] Gloria González Fuster, 'Article 80. Representation of Data Subjects', *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2020).
[151] González Fuster and others (n 147).
[152] Hakkarainen (n 47).
[153] ibid.
[154] Zuiderveen Borgesius (n 15); René Mahieu and Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' 1.

Similarly, a risk assessment procedure under the Digital Services Act (DSA)[155] is expected to influence AI development (of recommender and advertising systems, content moderation, etc.) in the context of very large online platforms and search engines.[156] Whilst the existence of these new legal obligations could foster further research on (intersectional) discrimination issues arising from the use of AI, fairness metrics and other techniques or organisational measures to address it, etc., their coordination remains uncertain.[157]

Another issue, apparently technical but with significant practical implications, depends on the lack of consensus as to the exact meaning of fairness, and the relationship thereof with non-discrimination, both in the computer science and legal communities. Whereas technical tools, including fairness metrics, can be useful to detect and address bias, guidance from legislators, regulators and possibly courts of law is also necessary to prevent the implementation of such instruments, whose effects on fundamental rights are so significant, evading democratic and judicial scrutiny.[158] It was mentioned above how various fairness metrics are possible. Whereas group fairness aims to ensure that groups differing in their sensitive attributes are treated equally, the goal of individual fairness is to avoid individuals being treated unfairly compared to other individuals. Yet, group fairness metrics may be unable to detect unfair outcomes on individuals, and *vice versa*.[159] Also, a fairness metric may work with regards to individual grounds individually considered, but not intersectionally. Thus, depending on the definition of what is *fair*, the results change dramatically.

In sum, although data protection law in the abstract could support the prevention of intersectional discrimination arising from personal data processing and facilitate the enforcement of intersectional discrimination claims, to make it more effective, it would be necessary to first overcome some structural limitations thereof. Suggestions made by scholars include improving the GDPR enforcement, by increasing transparency as to the use of automated decision-making systems, especially by the public sector, as well as possibilities for their audit by the public and independent experts and researchers; increasing the powers of DPAs and equality bodies;[160] not considering data subjects as a uniform group;[161] and strengthening the role of NGOs and collective actions for their empowerment.[162] Also (impact) assessments (e.g., DPIAs, or algorithmic impact assessment) could be helpful in preventing (intersectional) discrimination, provided that they reflect more broadly on the

[155] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). OJ L 277, 27.10.2022, p. 1–102.
[156] Calvi and Kotzinos (n 37).
[157] ibid.
[158] Wachter, Mittelstadt and Russell (n 21).
[159] Makhlouf, Zhioua and Palamidessi (n 35); Zuiderveen Borgesius (n 15).
[160] Zuiderveen Borgesius (n 15).
[161] Malgieri and González Fuster (n 59); Kadiri (n 64).
[162] van der Sloot and van Schendel (n 131); González Fuster and others (n 147).

persons and not just the type of data involved. Yet, to be truly effective and counterbalance the discretionality of the entities supposed to carry them out, they would need to be coupled with rights and remedies for impact assessment-related violations, transparency measures and periodic independent auditing.[163] Participation of the public and external experts in these assessments, as well as in technology development in general, has also been recommended.[164]

## 4. Conclusions

Both anti-discrimination and data protection laws in the EU are constantly evolving (data protection law at a faster pace than anti-discrimination law) to try to cope with new realities brought about by technological developments. In general, both legal frameworks strive to protect individuals and groups who are more at risk of being harmed (either through certain discriminatory behaviours or data processing operations) due to certain characteristics connoting them. In particular, data protection law has the merit of having created a framework for the more secure use of information, including sensitive data, to, for instance, prevent and address bias in automated systems, draw equality statistics, or measure the effectiveness of positive actions undertaken by Member States.

Both data protection and anti-discrimination laws have strengths and weaknesses which, to a certain extent, complement each other. For instance, the risk-based approach grounding the GDPR could enable circumventing the strict scope of the letter of Article 9 GDPR and, indirectly, expand the protected grounds under EU anti-discrimination secondary law. Such a broad approach to the notion of special categories of data seems confirmed by the case law of the CJEU. At the same time, the existence of grounds protected in anti-discrimination law but not reflected in the special categories of data could promote a better understanding of the risks brought about by the processing of certain types of information despite not being formally considered as a special category; as well as how the empowerment of data subjects within the processing (e.g., in exercising rights) may be affected by certain characteristics of the said data subject.

Even recent legislative developments currently under discussion within the EU institutions, such as the AIR, seem aware of the interrelationships between data protection and non-discrimination. In particular, Article 10(5) AIR appears to hold promise for the configuration of the substantial public interest exception *ex* Article 9(2)(g) GDPR, although, due to current technical constraints, the benefits thereof for intersectional discrimination cases remain rather theoretical. Further research as to the operationalisation of intersectionality in AI and fairness metrics is needed. The existence of data subject rights directly actionable against a controller could contribute to remedying the enforcement gap of intersectional claims in front of

[163] Calvi and Kotzinos (n 37).
[164] ibid.

courts. In parallel, the existence of legal remedies under anti-discrimination law could help cope with the compliance and enforcement deficit in data protection matters (although for intersectional discrimination claims this could be of little use). Data protection law, through for example the rights to access and transparency, may make visible certain otherwise invisibilised algorithmic discrimination cases.

Yet, some criticalities of data protection law in relation to (intersectional) discrimination remain. Attributing enhanced protection to special categories of data has proved to be a double-edged sword, in so far as, controllers often refrain from collecting sensitive data simply to avoid incurring extra administrative burdens. Further, special categories of data do not exhaust the categories of information that can be used to discriminate. Legal obligations mandating the processing of special categories of data for, e.g., equality monitoring, may exist at a national level, but they are relatively scarce and scattered. Thus, greater coordination between the two sectors, and possibly between data protection and equality bodies, is required to avoid reciprocally undermining data protection and anti-discrimination goals. Furthermore, the possibility for controllers to rely on a legal obligation to process sensitive categories of data, to a certain extent undermines data subjects' autonomy, especially because such a solution does not solve the lack of trust that data subjects may have in controllers holding their sensitive information. Indeed, controllers remain in the position of discriminating against data subjects, notwithstanding any good intentions. Promoting the processing of special categories of data by trusted third parties, or the use of synthetic datasets, could help but these measures are not exempt from criticism, as they still presuppose the collection of sensitive information.

Despite being considered a cornerstone for the protection of fundamental rights, even beyond data protection, the GDPR does not adopt a truly innovative approach towards intersectionality and intersectional discrimination issues. Concerns have also been expressed over the approach followed by the AIR, which is considered excessively focused on debiasing technologies instead of on the broader context of technology development. Indeed, despite part of the legal scholarship challenging this view, the GDPR still builds upon a liberal individualistic understanding of the right to personal data protection and of the notion of the data subject, which in turn affects the enforcement mechanisms foreseen under the Regulation. Collective actions under the GDPR remain largely underexplored, whilst actions in the name of an abstract interest in interest personal data protection seem forbidden.

The effectiveness of data protection law to tackle intersectional discrimination issues remains largely demanded by the goodwill of data controllers and the initiative of data subjects. The former can adopt, for instance, *ex ante* measures (e.g., DPIA, technical and organisational measures) and monitor their effectiveness discrimination-wise, be as transparent as possible concerning the logic behind the automated systems employed to favour external scrutiny, involve data subjects and their representatives in their decision-making concerning (impact) assessments, and follow up on data subjects' requests. Yet, controllers are already at the top of the 'data processing power chain', and the possibilities for DPA to investigate the GDPR-

related violations on the implementation of *ex ante* tools are rather limited. The latter can undoubtedly benefit from the *ex ante* protection tools set up by controllers, when available, and are also granted *ex post* remedies in the form of data subjects' rights. Yet, to demand their enforcement, data subjects are required to be materially able to exercise data subjects' rights (which entails, e.g., being capable of deciphering data protection notices, being aware of the existence of data subjects' rights and scope thereof, and being persistent in case of non-compliance). At the same time, notwithstanding that the AIR aims to be a functional instrument for the protection of fundamental rights (among the specific objectives thereof, to 'ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values' and 'enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems'), it does not contain any provision equivalent to data subjects' rights. Thus, even if the GDPR could be functional for the detection and enforcement of intersectional discrimination, it is not a silver bullet, due to, among other reasons, its limitations. However, as mentioned above, the two fields of data protection and non-discrimination are in constant evolution, meaning that the analysis is to be continued.