European Journal of Law and Technology, Vol 9, Issue 3, 2018

EJLT European Journal of **Law and Technology**

The Price Is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms

Laura Drechsler, Juan Carlos Benito Sánchez[1] [2]

Abstract

In the age of the large-scale collection, aggregation, and analysis of personal data ('Big Data'), merchants can generate complex profiles of consumers. Based on those profiles, algorithms can then try and match customers with the highest price they are willing to pay. But this entails the risk that pricing algorithms rely on certain personal characteristics of individuals that are protected under both data protection and anti-discrimination law. For instance, relying on the user's ethnic origin to determine pricing may trigger the special protection foreseen for sensitive personal data and the prohibition of discrimination in access to goods and services. Focusing on European Union law, this article seeks to answer the following question: What protection do data protection law and anti-discrimination law provide for individuals against discriminatory pricing decisions taken by algorithms? Its originality resides in an analysis that combines the approaches of these two disciplines, presenting the commonalities, advantages from an integrated approach, and misalignments currently existing at the intersection of EU data protection and anti-discrimination law.

Keywords: pricing algorithms, discrimination, data protection law, anti-discrimination law, European Union law

1. Introduction

It is no secret that different users are regularly shown different prices online. Algorithms determining these prices are ubiquitous in the online environment, where merchants are able to process unprecedented amounts of personal data and generate complex profiles of consumers. Pricing decisions can have a real impact on human lives, for instance when they concern credit applications, insurance premiums, or mortgage loans, and affect the ability of individuals to participate economically in our society. However, due to the opacity of algorithms, it is not clear on what basis prices are set for different individuals. There is an obvious risk that these pricing decisions are ultimately based on grounds which anti-discrimination law prohibits, like ethnic origin or gender.

From a legal scholar's point of view, the core question regarding potentially discriminatory pricing algorithms is whether the law provides any protection or remedies. Although the issue of 'price

discrimination' via algorithms has been dealt with in academic literature from the standpoint of how these algorithms are designed and in relation to the General Data Protection Regulation (GDPR), an enquiry into how anti-discrimination law specifically interacts with data protection law in this context remains crucial to understand how individuals are protected in their access to goods and services. This is particularly relevant in the European Union (EU) context, where both data protection and non-discrimination are considered fundamental rights.

In this article we set out to answer the following core question: What protection does EU data protection and anti-discrimination law currently provide against discriminatory pricing algorithms? In a first step, we establish what kind of protection EU data protection law and EU anti-discrimination law offer separately in this regard. Taking our analysis further, we elaborate on the commonalities, potential advantages of an integrated approach, and misalignments arising at the intersection of data protection and non-discrimination. To conclude our article, we bundle our arguments together and consider the broader implications of the interaction between these two fields of law through the example of pricing algorithms.

While we will look at the legal protection against discriminatory pricing algorithms from the perspective of EU data protection law and EU anti-discrimination law, a third area of EU law, namely EU consumer protection law,[3] might also be of relevance as it offers tools to protect against the imbalance between merchants and individuals, ranging from enhanced transparency (e.g. pre-contractual information obligations or requirements for price indications)[4] to contractual remedies addressing non-conformity of an acquired good or service with the contract.[5] However, an in-depth analysis of the interrelation between EU consumer protection law and discriminatory pricing algorithms would exceed the scope of this article and will therefore not be discussed here.[6]

1.1 Preliminary remarks: Price discrimination and algorithms

The term 'price discrimination' is regularly used in different contexts. From an economic point of view, the concept describes the process of matching customers with the highest price they are willing to pay.[7] It is pricing a product in a way that takes the personal attributes of the potential customer into account.[8] From that economic perspective, price discrimination is desirable insofar as it creates a better match between offer and demand, which could potentially be beneficial for the aggregated welfare.[9] In the field of competition law, pricing discrimination is used to explore the exploitative, distortionary, or exclusionary effects of certain commercial practices: price discrimination can be part of collusion or price fixing, and hence anticompetitive and a distortion for the market.[10]

In this article, we understand price discrimination from a data protection and an anti-discrimination law point of view. Price discrimination therefore means, for our purposes, the situation whereby the price of a product or a service varies depending on the personal information of users which the supplier of the product or service has available.[11] By price in this context we do not only mean the retail price in a sale, but more generally any monetary cost that individuals have to bear to obtain a good or service, including insurance premiums, loan interest rates, etc. Thus, price discrimination signifies for us using information that reveals individual characteristics in order to determine monetary costs.

Algorithms present the technological opportunity to track and monitor individuals. This is enabled by the large-scale collection, aggregation, and analysis of personal data,[12] or in other words the

use of 'Big Data'.[13] Pricing algorithms often use these techniques to try to achieve a better match between the price established by the merchant and the price a particular customer is willing to pay to acquire the particular good or service. The customer is 'scored' in order to be shown the 'right' price depending on his or her profile.

Pricing algorithms can be found in online retail stores (e.g. Amazon experimented with pricing algorithms in 2000),[14] the determination of insurance premiums and benefits (e.g. for a car or life insurance),[15] and mortgage and consumer loans (an algorithm might decide which interest rate and fees to show individuals initially).[16] Even though their use can result in economically rational matching between offer and demand, pricing algorithms can also lead to targeting specific types of customers while excluding others. Such profiled targeting can result in discriminatory outcomes if it leads to different prices, premiums, or rates for individuals based on prohibited grounds.[17]

While it is sometimes argued that assessing individuals through algorithms actually prevents discriminatory results, since 'unbiased' machines are less prejudiced,[18] it must be kept in mind that algorithms are not neutral, since they are programmed by people for people.[19] Additionally, the databases sourcing these algorithms can contain flawed information entered by biased individuals.[20] It is also important to note that the outcomes of algorithms reflect probabilities or correlations and not actual causation chains.[21]

Consequently, the use of pricing algorithms does not alleviate concerns that they might rely on prohibited grounds of discrimination as variables potentially hidden in the 'black box' of the algorithm.[22] Through the pervasive use of large personal datasets, these algorithms aggravate the risk of discrimination against individuals, at the same time that their fundamental right to data protection may be compromised.[23] As the following sections will show, the use of pricing algorithms for price discrimination poses challenges for both antidiscrimination and data protection law.

2. Applicability of data protection law to pricing algorithms

Within the EU, several data protection instruments ensure that the processing of personal data—also by pricing algorithms—must be fair, lawful and transparent. These instruments are, in a non-law enforcement context,[24] the GDPR (applicable from 25 May 2018, succeeding the Data Protection Directive (DPD))[25] and the e-Privacy Directive (EPD).[26]

To assess whether these instruments have any relevance for questions concerning pricing algorithms and discrimination, it is first necessary to establish the applicability of EU data protection law in general. The two key concepts for such applicability are 'personal data' and 'processing of personal data'. The concept of 'personal data' in EU data protection law was firstly defined in Article 2(a) DPD and has been clarified in Article 4(1) GDPR. It includes any information with which someone can either be directly identified or become identifiable. According to the Article 29 Working Party (WP29), an important role in this context is played by 'identifiers', which are information that can render a person identifiable, such as a name or an IP address.[27]

In general, identifiability is context-dependent.[28] In *Breyer* the Court of Justice of the European Union (CJEU) considered dynamic IP addresses personal data, since for the particular controller in that case (an online media service provider) it would have been possible to identify the person

behind them.[29] Thus, the concept of personal data has a very broad scope and it matters which resources a controller theoretically has at his or her disposal.[30] It has been argued that decisions made by (pricing) algorithms could potentially fall outside the scope of EU data protection law if anonymous data are used.[31] While it is conceivable that some algorithms may rely solely on anonymous data and produce decisions that cannot be linked to an identified individual (e.g. identification via keystroke dynamics),[32] this is usually not the case with pricing algorithms, which operate based on profiles.[33] Considering that these profiles often include information like IP addresses, location, or device fingerprints, we believe it safe to assume that they will normally resort to personal data to some extent in order to arrive at their pricing result.[34] Hence, we argue that the first condition for the applicability of EU data protection law seems to be fulfilled for pricing algorithms.

The concept of 'processing of personal data' is equally broad. According to Article 4(2) GDPR it means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration or otherwise making available, alignment or combination, restriction, erasure or destruction'. Processing performed by a pricing algorithm will usually fall within this definition, as it includes collection of data from as many sources as possible, analysis of such data, and the making available of the result of the analysis in the form of a price.[35] Therefore the second element for the applicability of EU data protection law is also fulfilled.[36]

Regarding the territorial and material scope of EU data protection law, regulated in Article 3 GDPR, it suffices that the establishment of the controller or the processor is within the EU and that the activity falls within Union law.[37] Territoriality is also fulfilled if a EU subject is targeted or is monitored.[38] Considering that pricing algorithms operate when goods and services are requested, the GDPR will almost always apply if a EU data subject is concerned, regardless of the establishment of the controller.[39]

The fact that EU data protection law applies in principle to pricing algorithms does not mean that it prohibits *per se* such algorithms.[40] In general, EU data protection law does not provide an *ex ante* choice to individuals about whether or not they want their data to be processed (in some cases, data subject rights give the possibility to object to the processing or to delete some results of processing *ex post*).[41] The only exception is the choice whether or not to consent in cases where the lawful basis for the processing is individual consent (which is only one out of six legal bases enumerated in Article 6 GDPR).[42] Additionally, even in consent situations, the individual cannot choose who is allowed to process their personal data once consent is given if the processing is covered by the original purpose of collection.[43] The processing of data in pricing algorithms can thus be perfectly legitimate, as long as the GDPR and potentially other secondary EU legislative norms regarding data protection are complied with.

The applicability of EU data protection law with regard to pricing algorithms results in the applicability of EU data protection principles, now neatly enumerated in Article 5(1) GDPR. These principles include *inter alia* the requirements of transparency and fairness, which are relevant for the use of algorithms and for concerns about discrimination. The principle of transparency is especially important for pricing algorithms.[44] Transparency means that data subjects must be in a position to understand how their actions influence the results of the algorithm. In other words,

they must be informed about the basic logic behind the workings of the algorithm.[45] The principle of transparency also demands that data subjects be aware of the personal data collected about them and that they be able correct inaccurate data.[46] The principle of fairness has a less clear scope, even though it is a fundamental principle of the GDPR and data protection in general.[47] According to Clifford and Ausloos the principle overarches the GDPR and encompasses many aspects, ranging from transparency to protection from power imbalances, and it can be summarised in the concepts of fair balancing and procedural fairness.[48] Considering the mere applicability of data protection law to pricing algorithms, this section concludes that data protection law is indeed applicable to pricing algorithms, but does not prohibit them as such.

3. Applicability of anti-discrimination law to pricing algorithms

Pricing decisions taken by algorithms can be problematic from an anti-discrimination law perspective. By determining the monetary costs that individuals have to bear to obtain a particular good or service, pricing decisions have an impact on the access of individuals to the market. According to anti-discrimination law, this access cannot be made dependent, generally speaking, upon certain characteristics such as racial or ethnic origin, gender, disability, sexual orientation, age, etc. Consequently, if an algorithm takes any of these factors into account to make a pricing decision that is then presented to an individual, that decision may be considered discriminatory and therefore be prohibited.

Some examples may help further illustrate this point. For instance, an individual living near a mosque and who regularly consumes halal products or books in Arabic could be categorised by an algorithm as belonging to an ethnic minority and potentially be offered different pricing from that of the ethnic majority. An applicant for a mortgage loan may experience higher interest rates because they live in a neighbourhood mostly inhabited by people of a particular ethnic origin, independently of whether the applicant belongs to that group or not. A young woman may face higher insurance premiums for health care on the basis of her gender and age, since the algorithm may take into account the higher costs usually associated with pregnancy.

Under EU law, the notion of access to goods and services has been interpreted in a large sense, as covering a wide range of activities ranging from banking, insurance, transport, or travel services to the business operation of cinemas, hotels, or restaurants.[49] It applies to all goods and services 'which are available to the public and which are offered outside the area of private and family life and the transactions carried out in this context'.[50] This means that a pricing decision taken by an algorithm in the framework of these activities will generally come under the scope of anti-discrimination law, since it concerns goods and services available to the public.

According to anti-discrimination law, a pricing decision product of an algorithm will be discriminatory—and therefore prohibited—if it has been taken 'on the basis of' one of the prohibited grounds (direct discrimination), or if it has a disproportionate impact on certain groups defined by a prohibited ground without an objective and appropriate justification (indirect discrimination).[51] In other words, in order to comply with anti-discrimination law, merchants ('controllers' for EU data protection law) must ensure that certain data related to immutable characteristics or fundamental choices of individuals are not used as the basis to take pricing decisions, and that those decisions do not have a disproportionate impact on certain groups without an adequate justification. Direct discrimination is linked to a more stringent regime, as it cannot in principle be justified, whereas indirect discrimination allows for more flexibility in terms

of justification.

For the purposes of this article, we focus on direct discrimination as the most immediate type of discrimination likely to emerge from pricing decisions taken by algorithms. Direct discrimination applies to the situation where personal data relating to one or more of the prohibited grounds is embedded in the 'black box' of the algorithm, and is used to take a pricing decision. Even if this data linked to prohibited grounds is only used in part by the algorithm to determine the final outcome, that partial use will taint the decision with discrimination, insofar as it will be considered as taken 'on the basis of' a prohibited ground.

However, indirect discrimination is also conceivable in these situations if an algorithm uses criteria which, although facially neutral and unrelated to any of the prohibited grounds, have a disproportionate impact on some protected groups without an adequate justification. One could think, for example, of an online retail store using an algorithm to take pricing decisions on the basis of the user's browser agent. If a significant number of users in a specific age bracket (say, 60+ years old users) use the same legacy web browser on dated computer equipment, and see higher prices as a consequence, a case might be made for indirect age discrimination. However, indirect discrimination cases will generally be less frequent and harder to prove than direct discrimination cases.

At the EU level, discrimination (both direct and indirect) in the access to goods and services is prohibited on the grounds of gender and of racial or ethnic origin.[52] For instance, if an algorithm establishes higher prices for women than men on account of the user's gender, this will be considered discriminatory. Although the Charter of Fundamental Rights forbids in its Article 21 any discrimination 'based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation', this provision does not extend the field of application of Union law, and cannot be used as such to expand the prohibition of discrimination in access to goods and services to other grounds.

The case of insurance premiums and benefits illustrates well this discussion. The Gender Goods and Services Directive explicitly mentions that 'the use of sex as a factor in the calculation of premiums and benefits for the purposes of insurance and related financial services shall not result in differences in individuals' premiums and benefits'.[53] Consequently, if an algorithm determines premiums and benefits on the basis of sex—even if this criterion is only used in part for that determination—, the resulting pricing decision will breach antidiscrimination law. In the seminal case *Test-Achats*, the Court of Justice clarified this prohibition and confirmed that it is no longer allowed within the EU to treat male and female policyholders differently when calculating premiums and benefits for insurance contracts, and this on account of the principle of equality and non-discrimination enshrined in Articles 21 and 23 of the EU Charter of Fundamental Rights.[54]

It could be argued that this prohibition extends, in the EU context, to racial or ethnic origin. According to the Race Equality Directive, discrimination on the basis of racial or ethnic origin is also prohibited with regard to access to goods and services.[55] A consistent interpretation of EU law would lead us to the conclusion that racial or ethnic origin cannot either be a factor for the calculation of premiums and benefits for the purposes of insurance and related financial services. In the words of Advocate General Kokott:

The Council may not therefore, for example, permit a person's race and ethnic origin to be used as

a ground for differentiation in insurance. In a Union governed by the rule of law, which has declared respect for human dignity, human rights, equality and non-discrimination to be its overriding principles, it would without doubt be extremely inappropriate if for instance, in the context of medical insurance, varying risks of contracting skin cancers were to be linked to the skin colour of the insured person and either a higher or lower premium were thus to be demanded of him.[56]

Pricing algorithms, as established above, affect the ability of individuals and groups to access goods and services. If the monetary cost incurred to access these goods or services is determined on the basis of gender or of racial or ethnic origin, that decision will constitute direct discrimination under EU law, which is prohibited. This is especially relevant in the case of insurance, where algorithms ordinarily take into account actuarial factors in order to calculate premiums and benefits.[57]

Moreover, national legal orders often extend this prohibition of discrimination in access to goods and services to cover additional grounds, like a person's habits, place of residence, or even the particular vulnerability resulting from their economic situation.[58] In Belgium, for instance, discrimination in access to goods and services is prohibited on account of nineteen criteria, among which national origin, disability, sexual orientation, wealth, or health status.[59] This may lead to questioning the discriminatory dimensions of many pricing decisions taken by algorithms that would be otherwise not relevant from an anti-discrimination law perspective.

To sum up, EU anti-discrimination law applies to pricing algorithms insofar as they have an impact on the access of individuals to goods and services. At the EU level, discrimination in the access to goods and services is only prohibited with regard to racial or ethnic origin and gender, although national law may contain a more comprehensive protection and include additional grounds.

4. Data protection law meets anti-discrimination law: Commonalities, potential advantages of an integrated approach, misalignments

4.1 Commonalities of data protection and anti-discrimination law

As this article offers an analysis from both EU data protection and anti-discrimination law, it seems useful to consider whether these two fields of law share any concepts or have any clear interconnections. Our research revealed three such 'obvious' intersections: first of all, the notion of fairness lies at the core of both data protection and anti-discrimination.[60] Secondly, the special protection of certain elements revealing potential discrimination features in both areas of law. For data protection law these elements can be found in special categories of data, also called 'sensitive data'.[61] For anti-discrimination law, these elements are embodied by prohibited grounds. There is a substantial overlap between these two categories. Finally, the special rules on automated decision-making in EU data protection law clearly stem from discrimination concerns.

4.1.1 Fairness

Fairness as a concept is hard to define. From a data protection perspective, it is clear that within the EU the processing of personal data needs to be 'fair',[62] but it remains elusive what 'fair processing' actually entails.[63] A detailed analysis of this concept is far beyond the scope of this article. For our purposes, it suffices to say that fairness entails the notion that data subjects should be treated fairly.[64] As Clifford and Ausloos argue, this does not only mean that data subjects must not be deceived by the controller about what is happening with their personal data, but it also aims at counterbalancing the inherent imbalance in data protection between data subject and controller in a more general manner.[65]

Data protection and anti-discrimination law do not only share this initial aim of re-establishing fairness, they also go in similar ways about it. As Gellert et al. note in their comparison of data protection and anti-discrimination law within the EU, both areas of law stipulate legal principles and establish administrative bodies (data protection authorities and equality bodies), as well as individual rights for the affected (data subject rights and access to justice rights).[66]

A final commonality between anti-discrimination and data protection law achieved through the notion of fairness lies in the concept of 'fair balancing', which for Clifford and Ausloos forms one core string of fairness, and represents the need for necessity and proportionality to be examined when there is a clash with other fundamental rights.[67] This aspect of fairness was also pivotal when the CJEU discussed its so far only case mentioning[68] both data protection and non-discrimination: *Huber*.[69] In *Huber*, an Austrian living in Germany complained about his inclusion in a German database for foreigners that was much more comprehensive that any database on German nationals. In his complaint, he claimed that he had been discriminated against on the basis of nationality. The CJEU analysed the facts mainly from a data protection angle, but considered discrimination within the data protection analysis when examining the necessity of the processing, which was 'interpreted in the light of the prohibition on any discrimination on grounds of nationality'.[70]

In light of the above, we argue that data protection and non-discrimination are two fundamental rights working towards the same goal through the notion of fairness. Hence, unlike some other fundamental rights pairings, such as data protection and freedom of expression, they do not require balancing but rather inform each other's interpretation, as can be tentatively seen in *Huber*.

4.1.2 Sensitive data and prohibited discrimination grounds

Sensitive data are defined in Article 9(1) GDPR as so-called 'special categories of personal data'. It includes all personal data linked to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data and biometric data if used to uniquely identify a person, health data, and data concerning a person's sex life or sexual orientation. The processing of sensitive data is in principle prohibited under EU data protection law.[71] Sensitive data are considered especially worthy of protection due to their close connection with various fundamental rights[72] and their high risk for potential discriminatory outcomes.[73] The WP29 considers that using such data in algorithms, such as those used for

behavioural advertising, poses a serious risk to the right to personal data protection of individuals. [74]

Due to this higher risk of discrimination and violation of other fundamental rights, EU data protection law has always prescribed special rules for the processing of sensitive data, starting from the general prohibition thereof. Taking the GDPR as the latest example of data protection legislation, while sensitive data require a specific legitimate basis to be processed (just as non-sensitive personal data), these bases are more limited in their application. The legitimate bases of Article 9(2) GDPR are therefore more strict compared to the ones enlisted in Article 6(1) GDPR, though overlaps can occur.[75]

The protected categories for sensitive personal data according to Article 9(1) GDPR are from the outset similar to the protected grounds of EU anti-discrimination law.[76] Differences exist however,[77] considering that neither gender nor age are considered sensitive data in EU data protection law. While age can in some instances be linked to health data and thus profit from the special protection for sensitive data, the processing of data about gender will generally fall outside this special regime. This is especially unfortunate since gender is one of the two protected grounds on the basis of which EU anti-discrimination law condemns discrimination in the access to goods and services—the other ground being racial or ethnic origin. Combining the general prohibition of processing sensitive data with the limited catalogue of exceptions for processing could lead to the conclusion that anti-discrimination law and data protection law are sufficiently aligned. However, this is not the legal reality.

First, the limited catalogue of exceptions includes the explicit consent of the data subject, which is, according to Zuiderveen Borgesius and Poort, the only realistically possible legitimate basis for the processing of sensitive data by a pricing algorithm.[78] Compared to the 'normal' consent of Article 6(1)(a) GDPR, 'explicit' consent requires that the consent specifically relates to the fact that sensitive data are being processed.[79] In addition, the GDPR provides the opportunity for Member States and other Union legislative acts to exclude certain forms of sensitive data processing from this legal basis.[80] While these precautions heighten the threshold for consent, they do not alleviate the fact that people readily consent away their (sensitive) data.[81] On the other hand, as Zuiderveen Borgesius and Poort note, due to the unpopularity of pricing algorithms their reliance on consent as a legitimate basis for the processing of sensitive data seems difficult in practice, should the data subject/consumer be aware of what is going on.[82]

Second, as shown above, not all prohibited grounds represent at the same time sensitive data. Hence, relying solely on the strict regime for sensitive data to protect individuals from discriminatory pricing algorithms would not be helpful in combatting discrimination based on gender, and, potentially (at the national level), age.

To summarise, while the special legal regime for sensitive data—which is actually based on the heightened risk of discrimination—offers some protection against discriminatory pricing algorithms, this does not *per se* offer a satisfactory solution. In any case, the fact that sensitive data are afforded stronger protection because of the increased risk that they lead to discrimination shows that the EU legislator acknowledges the interconnection between data protection and non-discrimination.[83]

4.1.3 Automated decision-making and Article 22 GDPR

Article 22 GDPR establishes a 'right' not to be subject to automated decision-making without any human intervention that results in legal effects or similar other effects for the data subject. The aim of this provision is explained in Recital 71 of the GDPR, which puts on the controller the obligation to secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, *discriminatory effects* on natural persons on the basis of racial or ethnic origin, political opinion, religion or belief, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect (emphasis added).

Article 22 is not an invention of the GDPR, but was already included in the DPD with very similar wording but limited practical success.[84] This unsuccessfulness can be partly attributed to the ambiguity of the formulation of Article 15 DPD (unfortunately left unchanged in Article 22 GDPR), [85] mentioning 'a right not to be subject to'. As Wachter et al. explain, this can be interpreted either as a prohibition of solely automated decisions without human intervention to which controllers have to comply *ex ante*, or a subjective data subject right (a sort of additional right to object) that can be invoked by the concerned individual.[86] Naturally, the first interpretation offers more protection than the second, as it would not depend on any action by the data subject. [87]

While the GDPR also stipulates a *right not to be subject to*, continuing the confusion of Article 15 DPD, the WP29 clearly states in its guidance on Article 22 that 'the term "right" in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing'. [88] Unfortunately, the guidance provided by the WP29 is not binding, so it will be up for the CJEU to authoritatively decide what Article 22 exactly entails.[89]

More problems stem from the scope of application of Article 22, which includes only decisions 'based solely on automated processing […] which [produce] legal effects concerning him or her or significantly [affect] him or her'.[90] The fact that Article 22 GDPR refers to a 'solely automated decision' could be interpreted as meaning that any type of human intervention renders the provision inapplicable.[91] However, according to Voigt and von dem Bussche human involvement can only be considered when it is connected to decision-making powers; in other words, the human involved must be able to influence the content of the final outcome.[92] This interpretation was confirmed by the WP29.[93]

Further issues are created by the condition that the automated decision must produce legal or similarly significant effects. According to some authors, this condition means that Article 22 GDPR only applies for example, in the context of pricing, when algorithms lead to significantly higher monetary costs for the data subject (hence not for reductions or small differences in pricing).[94] As the GDPR does not specify these legal or similar effects, much will again depend on the interpretation of the CJEU. For other authors, it seems likely that the provision of Article 22 GDPR will apply to most pricing algorithms: for instance, 'price discrimination' is listed as an example by Malgieri and Comandé.[95] This opinion is also shared by the WP29, which considers both the 'affecting of someone's financial circumstances such as their eligibility to credit' and the 'automatic refusal of a credit application' as examples for legal or similarly significant effects.[96]

Article 22 GDPR also includes a special regime with regard to the processing of sensitive data.

According to Article 22(4) GDPR this 'right' concerning automated individual decision-making is always applicable if sensitive data are being processed. Article 22 GDPR therefore entails a general prohibition of automated decision-making based on sensitive data, following the WP29 guidance. [97] This prohibition knows only two exceptions: when the processing of the sensitive data was based on explicit consent and when the processing was based on a substantial public interest. Recital 71 highlights that 'automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions'. However, even if one of these two exceptions apply, the processing can only take place with 'suitable measures' securing the data subject's rights and freedoms.[98] According to Malgieri and Comandé those measures include at least the right to obtain human intervention and the right to contest the decision.[99]

It follows therefrom that *if* Article 22 GDPR contains indeed a general prohibition of processing sensitive data for automated decision-making, *and* pricing algorithms fall within its concept of an automated decision producing legal or similarly significant effects, that provision could be a substantial protection against discriminatory pricing algorithms. We however consider that due to the large ambiguities regarding the function and scope of Article 22 GDPR, and while this provision reflects promising interconnections of non-discrimination and data protection, it currently fails to properly accommodate this link.[100]

4.2 Potential advantages of an integrated approach

As it can be gathered from the previous sections, neither EU data protection law nor EU anti-discrimination law alone seem to provide complete protection against pricing algorithms discriminating on the basis of protected grounds. Although commonalities between both legal regimes exist, this overlap does not extend to all situations. This is unsatisfactory, considering that both data protection and non-discrimination are considered fundamental rights at the EU level. Both of these rights call into question the supposed neutrality of certain algorithms, and highlight the fact that flawed information and bias can be hidden behind certain pricing decisions. In this section we explore areas where using a more integrated combination of EU data protection and anti-discrimination law could represent a way forward. Such a combination would be especially fruitful in cases where EU anti-discrimination law stretches beyond the limitations of EU data protection law, and vice-versa.

4.2.1 Data protection law offers transparency tools that facilitate proof of discrimination

As explained above, a pricing decision taken 'on the basis of' one of the prohibited grounds stated in EU anti-discrimination law will constitute direct discrimination. In our view, the process of making a claim of discrimination can be facilitated by one of the cornerstones of EU data protection law, namely EU data subject rights.

Data subject rights in EU data protection law aim to overcome the concerns linked to problems of transparency, which will also be present whenever pricing algorithms are involved.[101] Data subject rights secure the individual's right to have a voice in data processing about him or her. [102] The data subject rights of relevance for discriminatory pricing algorithms are those contributing to enhanced transparency, namely the right to information (Articles 13 and 14 GDPR) and the right of access (Article 15 GDPR).[103]

The GDPR introduced important clarifications with regard to the right to information of the data subject. Articles 13 and 14 prescribe that the data subject shall be informed *ex ante* 'about the

existence of automated decision-making, including profiling', and that they need to receive meaningful information about 'the logic involved, as well as the significance and the envisaged consequences of such processing'.[104] This is in line with the data protection principle of transparency, and should encompass nearly all pricing algorithms since, as we argued, they can be considered profiling by automated means since they rely to a certain extent on personal data of the individual.[105] As a consequence, such pricing algorithms not involving profiling (e.g. pricing algorithms for the stock market, which calculate the worth of a specific stock at a specific time) would not be included as long as they do not also involve some assessment of, for example, price sensitivities on the side of the prospective buyer, which again would require a certain amount of profiling (including insights on past price sensitivity, job, income, family situation, etc.).[106]

The right of access is meant as a tool for data subjects to verify the fairness and transparency of data processing concerning them.[107] Compared to the information rights of the data subject, it is a right to be used *ex post*, after the processing has occurred.[108] Article 15(1) GDPR lists under (h) an information obligation, meaning that an access request in the context of a pricing algorithm must be accompanied by information about the workings of the algorithm and possible consequences for the data subject.

While the amount of information that needs to be offered under Articles 13, 14, and 15 GDPR is heavily debated, even under the most restrictive view it is clear that some meaningful guidance on the workings of the algorithm must be included, even if it is more generic.[109] This could mean, for example, that an individual subject to credit scoring receives information on what datasets are considered positively and what datasets are considered negatively for his or her credit rate. This is comparable to law students receiving a grading scheme before an exam in order to be able to roughly assess what kind of answers will be graded in what way. While this can never guarantee a full prediction of the outcome, it can help the individual understand why the outcome is how it is. Such information could be sufficient to help prove discrimination if, for instance, it is shown that part-time work or a certain age are being used as negative factors.[110]

An integrated approach, in the sense of using these transparency rights to uncover discrimination, offers several opportunities. While anti-discrimination law is better equipped to address the wrong that occurs when algorithmic decisions on pricing are based on protected grounds, EU data protection law offers the tools needed to reveal that discriminatory practice. Data subject rights, such as the right to information and the right of access, could thus play an important role in obtaining evidence establishing that a decision by an algorithm is based on protected grounds. Moreover, since Article 80 GDPR now offers the possibility for data subjects to entrust their rights to a non-profit, organisation, or association, the door seems to be open for equality bodies to make use of data subject rights on behalf of victims of discrimination. We believe that such a combined approach could prove very successful in the future.

4.2.2 The use of proxies in data protection and anti-discrimination law

A second area where anti-discrimination law and data protection law could benefit from an integrated approach concerns proxies. We have discussed the situation whereby a merchant (controller) uses sensitive personal data related to prohibited discrimination grounds to take pricing decisions via an algorithm. However, what happens if a merchant (controller) does not process sensitive personal data, but uses the complex set of information they possess about a particular person to infer sensitive personal data? Many parameters can be used as a proxy for a

prohibited discrimination ground. For instance, a company may aggregate data such as the street or neighbourhood where individuals live and the type of products they consume to determine their racial or ethnic origin.[111]

As long as a decision is ultimately taken 'on the basis of' one of the prohibited grounds, this will constitute direct discrimination under anti-discrimination law. For instance, it has been shown how some mortgage lenders rejected loan applications or determined interest rates on the basis of the racial or ethnic origin of the applicants. This practice is known as *redlining*. As a result, black and Hispanic applicants were rejected or charged significantly higher rates than white applicants in the US.[112] Similar practices have also been documented in the European context.[113] Often, these decisions did not rely on the racial or ethnic origin of the applicants as such, but rather on the racial or ethnic origin of the majority of inhabitants in the particular neighbourhood or area where the applicants lived. In other words, an algorithm aggregated data concerning racial or ethnic origin as well as property values and other neighbourhood metrics, and provided a decision to accept or reject a loan or to set interest rates at a particular level. This decision, however, had been partly taken on the basis of racial or ethnic origin.

It is important to clarify that in these cases that the decision to reject an applicant or to charge higher interest rates will be considered direct discrimination. In the context of EU law, it is clear that direct discrimination will occur whenever a decision is taken on the basis of the origin of the majority of the inhabitants in a neighbourhood, even if the particular individual affected is not of the same origin. The Court of Justice clarified as much in the *CHEZ* case, stating that, even if the applicant in the particular case was not of Roma origin, 'it is indeed Roma origin, in this instance that of most of the other inhabitants of the district in which she carries on her business, which constitutes the factor on the basis of which she considers that she has suffered less favourable treatment or a particular disadvantage'.[114]

The treatment of proxies for sensitive data is similar in data protection law. On the basis of the sheer amount of personal data algorithms have at their disposal, proxies are likely to be found and used.[115] According to the EDPS, this leads to the risk that 'highly sensitive data […] can be predicted from seemingly non-sensitive information, such as […] key stroke dynamics'.[116] So far, the CJEU has been very strict about sensitive data and applied the special, more stringent regime to cases where proxies have been used,[117] allowing for the assessment that at least clear proxies for sensitive data are not sufficient to avoid the special safeguards EU data protection law foresees.

Combining the CJEU's strong stance on proxies in both areas could lead to even stronger protection against pricing algorithms. Additionally, both disciplines could rely on each other when trying to define the difference between a prohibited proxy and a nonrelated data item, which could potentially lead to inferences similar to proxies, depending on the means used.[118] We believe that a streamlining of legal regimes could alleviate the major evidentiary issue that the use of proxies reveals: proving when they have effectively been used.[119]

4.2.3 Anti-discrimination law as a means to counterbalance data protection's heavy reliance on consent

As we have explained so far, EU data protection law includes safeguards and opens potential venues to address discrimination by pricing algorithms. These safeguards include the more

stringent regime of protection for sensitive data and the potential general prohibition of automated decision-making without human intervention based on sensitive data. However, for both provisions consent is an exception and, unfortunately, consent has proven to be less of an insurmountable barrier in the past, as data subjects tend to consent without reading the details. [120]

The flaw from a data protection perspective for protecting individuals against discrimination by pricing algorithms thus lays in the heavy reliance of its remedies on consent.[121] While a motivated individual could use data protection tools to uncover discrimination, 'passive' individuals will not enjoy the same amount of protection in practice. Article 80 GDPR could be of some help here, as it introduces the possibility to 'mandate a not-for-profit body, organisation or association' with the exercise of the rights of the data subject. In this regard, some authors have suggested that third parties such as governments or NGOs could hold sensitive data related to prohibited grounds to facilitate this task.[122] Another possibility would be developing 'soft' policy initiatives such as certificates or labels to indicate to users whether their sensitive data are being used to determine pricing or to take other important commercial decisions. However, in the end all these tools rely on a certain active engagement of the individuals concerned.

The heavy reliance on consent and the 'privacy paradox', leading individuals to consent to different kinds of processing without knowing the details while at the same time being generally concerned about privacy and data protection, could be to a certain extent counterbalanced by anti-discrimination law. The injury of being potentially discriminated against based on a protected ground can lead to more awareness and a greater perception of injustice in individuals, who might therefore pay closer attention and use the tools data protection law provides them with.[123]

4.3 Misalignments between data protection and anti-discrimination law

As a final point in this section, it is important to note some misalignments of current anti-discrimination law and data protection law that we found in our research. First, it is sometimes argued that the detection of discriminatory bias in algorithms can only occur via the processing of sensitive data.[124] Especially Zarsky highlights that algorithms can only be tested for some types of discrimination by using sensitive data.[125] Anti-discrimination law scholars have similarly shown that the availability of such data is key to developing non-discriminatory policies and practices.[126] This raises the question whether such processing of special categories of personal data is permitted under the EU data protection regime.

Arguably, such processing for the general testing of algorithms could be permissible under either Article 9(2)(g) GDPR as 'processing that is necessary for reasons of substantial public interest, on the basis of Union or Member State law', or Article 9(2)(j) GDPR as 'processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes […] based on Union or Member State law'. Both would require further legislative steps by either the Member States or the EU.[127] For specific legal claims about discrimination through a pricing algorithm, Article 9(2)(f) could be the appropriate legal basis for the preparation of the legal claim for the court proceedings.[128] This legitimate basis is however only suitable for individuals preparing a concrete court action, and not for generally testing potential discrimination via pricing algorithms. None of the mentioned legal bases seems therefore obvious for general testing, especially when no individual has been previously affected.[129]

Another important respect in which EU data protection and anti-discrimination law are misaligned is the relationship between the categories of sensitive data and prohibited discrimination grounds. Even if these two categories overlap for the most part, certain grounds, in particular gender and age, are not in principle considered as sensitive data. As mentioned above, this misalignment risks creating gaps in protection from discrimination, both as regards the data protection provisions on sensitive data and the safeguards against automated decision-making contained in Article 22 GDPR. While there is no easy solution to this misalignment,[130] we hope that future research will more clearly elaborate on the link between sensitive data and discrimination

5. Conclusions

All things considered, it must be emphasised that the key issue here is that goods and services should be allocated to anyone willing or able to pay their price, and not according to personal circumstances. In other words, different treatment on the basis of different purchasing power is not the same as different treatment on the basis of data-driven judgments about who users are. [131] Generally, both anti-discrimination and data protection law concern themselves with discriminatory pricing algorithms and include them in their scope of application. However, on their own, neither provides adequate protection. A combined approach seems therefore necessary. [132]

Our research shows that, unlike many other fundamental rights, there is in principle no conflict or balancing required between data protection and non-discrimination. Quite the opposite: both seem to serve the same master of fairness, and are compatible and interlinked in their application and concepts. The core problem, in our opinion, lies not in any discrepancies between these two fields of law, but rather in the lack of an integrated legal regime.

As we have explained, using data protection tools in non-discrimination cases could be an effective way of satisfying the evidentiary threshold. Additionally, more streamlining on the legal treatment of proxies is needed. Finally, discrimination could help make individuals pay more attention to data protection issues, since most data protection safeguards currently rely on consent and/or the active engagement of the data subject. However, the integration of anti-discrimination and data protection law is not completely seamless, as there remain some misalignments.

Overall, we believe that due to the many shared values, an integrated approach towards anti-discrimination and data protection law would be capable of providing enhanced protection against discriminatory pricing algorithms. This is independent from the 'chicken-or-egg' question of whether pricing algorithms are essentially a data protection or a non-discrimination issue. We put forward that they are both. For strategic reasons, it might sometimes make more sense to approach a pricing algorithm from a data protection angle, as the scope of EU data protection law is wider and the evidentiary threshold lower, but even then any analysis cannot do without serious consideration of anti-discrimination law.

In the end, non-discrimination may be considered as an essential dimension to secure the fundamental right to data protection of individuals. Data protection cases involving pricing algorithms will often raise questions in terms of potentially discriminatory effects. At the same time, the effectiveness of anti-discrimination law is bolstered by data protection law, in particular through the additional tools and safeguards it foresees. These two disciplines provide a combined answer to those situations where, unlike in the popular TV entertainment show, the price is *not* quite right.

[1]PhD Researcher (FWO), Brussels Privacy Hub, LSTS, Vrije Universiteit Brussel (Belgium), laura.drechsler@vub.be; PhD Researcher (F.R.S.-FNRS FRESH), Centre de philosophie du droit, UCLouvain (Belgium), juan.benito@uclouvain.be

[2]This article was originally presented in its draft version at the Young Scholars Event 'Opening the Black Box of Technology: The Place of Fundamental Rights', organised by the Université Libre de Bruxelles and which took place in Brussels on 18 May 2018. We would like to thank the organisers and the participants for their useful feedback, as well as the EJLT anonymous reviewers for their comments.

[3] For the European Data Protection Supervisor (EDPS), consumer protection law, data protection law, and competition law should be streamlined to properly address challenges posed by big data technologies, including algorithms. For an overview of what EU consumer protection law can contribute to a more just online environment, see European Data Protection Supervisor, Preliminary Opinion: Privacy and competitiveness in the age of big data – interplay between data protection, competition law and consumer protection in the Digital Economy (March 2014): 23-26.

[4] More transparency for the consumer is ensured through the Directive on Unfair Contract Terms, requiring merchants to avoid confusing terms in consumer contracts; through the Price Indication Directive, setting standards on transparency for prices; and through the Consumer Rights Directive, introducing additional information requirements, especially for online services. See Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95 (21 April 1993); Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers, OJ L 80 (18 March 1998); Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC; and Directive 97/7/EC of the European Parliament and of the Council (Text with EEA relevance), OJ L 304 (22. November 2011).

[5] These remedies were introduced with the Consumer Goods and Guarantees Directive, which is currently being revised by the European legislator, and includes the remedies of repair, replace, reduce in price, and annulment of the contract. See Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171 (7 July 1999).

[6] For an analysis of the relationship between data protection and consumer law, see Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'A perfect match? A closer look at the relationship between EU consumer law and data protection law', *Common Market Law Review* 55 (2017):1427–1466.

[7] Richard Steppe, 'Online price discrimination and personal data: A General Data Protection Regulation perspective', *Computer Law & Security Review* 33 (2017): 769.

[8] Jakub Mikians, László Gyarmati, Vijay Erramilli and Nikolaos Laoutaris, 'Detecting price and search discrimination on the Internet', *Proceedings of the 11th ACM Workshop on hot topics in networks (HOTNETS-XI)* (2012): 79.

[9] It has however been argued that, generally, price discrimination will only enhance welfare if it is linked to substantial market expansion in markets that were previously unserved. See Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law', *Journal of Consumer Policy* 40 (2017): 355.

[10] The EDPS has stated that so far competition law has not adequately addressed discriminatory pricing concerns. Unfortunately, the EDPS has not included anti-discrimination law in its call for a greater streamlining of data protection law and other disciplines. See: EDPS, Privacy and competitiveness, 21.

[11] Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 348.

[12] Paul De Hert, Serge Gutwirth, Anna Moscibroda, David Wright and Gloria Gonzaléz Fuster, 'Legal safeguards for privacy and data protection in ambient intelligence', *Pers Ubiquit Comput* 13 (2009): 436.

[13] See definition of 'Big Data' in Richard Kemp, 'Legal aspects of managing Big Data', *Computer Law & Security Review* 30 (2014): 483, ' "Big Data" is therefore shorthand for the collection, processing, analysis and use of vast exploitable datasets of unstructured and structured digital information'.

[14] Mark Ward, 'Amazon's old customers "pay more," ' *BBC News*, September 8, 2000, http://news.bbc.co.uk/2/hi/business/914691.stm

[15] As Kemp describes, personal data gathered from various 'Big Data' applications, such as wearables or sensors, can influence the prices of insurance policies for cars, houses and health. See Kemp, 'Legal aspects of managing Big Data', 484-484.

[16] See Louise Matsakis, 'Your smartphone choice could determine if you'll get a loan', *WIRED*, May 8, 2018, https://www.wired.com/story/your-smartphone-could-decide-whether-youll-get-a-loan/amp?__twitter_impression=true See also DF-Xinhua Report, 'Discrimination through artificial intelligence banned', *Daily Finland*, April 26, 2018, http://www.dailyfinland.fi/national/5168/Discrimination-through-artificial-intelligence-banned See also Asiedu et al., who analysed discrimination in the access to credit for small business owners in the US and found discrimination against women and minorities. The decisions to grant credit are supported by algorithms creating credit scores. See Elizabeth Asiedu, James A. Freeman and Akwasi Nti-Addae, 'Access to Credit by Small Businesses: How Relevant are Race, Ethnicity and Gender?', *American Economic Review: Papers and Proceedings 2012* 102(3) (2012): 532-537.

[17] See Cassandra Jones Havard, 'On the Take: The Black Box of Credit Scoring and Mortgage Discrimination', *Pub. Int. L.J.* 20 (2011): 271, where she establishes a link between the U.S. subprime mortgage crisis and credit scoring based on race. See also Tal Z. Zarsky, 'Understanding Discrimination in the Scored Society', *Wash. L. Rev.* 89 (2014): 1384. Within the EU context, the Fundamental Rights Agency (FRA) warned in a recent opinion about the dangers of direct and indirect discrimination via algorithms. See: European Union Agency for Fundamental Rights, #BigData: Discrimination in data-supported decision-making (2018): 3.

[18] Danielle Keats Citron and Frank Pasquale, 'The scored society: Due process for automated predictions', *Wash. L. Rev.* 89 (2014): 4-5.

[19] See Michael Veale and Reuben Binns, 'Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data', *Big Data & Society* (July-December 2017): 2. See also the law of computing 'garbage in–garbage out' as explained in: World Economic Forum, White Paper: How to prevent discriminatory outcome in machine-learning, Global Future Council on Human Rights 2016-2018 (March 2018): 9.

[20] Citroen and Pasquale, 'The scored society', 13-14; Zarsky, 'Understanding Discrimination in the Scored Society', 1390-1393; Indre Zliobaite and Bart Custers, 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models', *Artif Intell Law* 24 (2016): 184. See also the resolution of the European Parliament warning explicitly about the risks of flawed data in a European context, European Parliament, Fundamental rights implications of big data, P8_TA(2017) (14 March 2017): M.

[21] FRA, #BigData, 4.

[22] See Citroen and Pasquale, 'The Scored society', 24. See also, using the example of US credit scoring, Havard, 'On the Take', 250.

[23] Belleflame and Vergote even suggest that data subjects taking privacy-protecting measures are being charged higher prices for remaining unidentified, see Paul Belleflame and Wouter Vergote, 'Monopoly price discrimination and privacy: The hidden cost of hiding', *Economics Letters* 149 (2016): 141-144.

[24] For the area of law enforcement, the EU established specific rules in Directive 2016/680, which follows the same data protection principles as the GDPR but focuses on the specificities of the law enforcement context. See: European Union, Directive (EU) 2016/680 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 May 2016).

[25] European Union, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data, OJ L 291 (23 November 1995). While this article includes some references to the DPD, mainly to demonstrate the origins of different data protection concepts, the bulk of the analysis will focus on the GDPR.

[26] Directive 2002/58 of 12 July 2002 concerning the processing or personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (as amended by Directive 2006/24/EC and Directive 2009/136/EC), OJ L 337 (18 December 2009).

[27] Article 29 Data Protection Working Party (WP29), Opinion 4/2007 on the concept of personal data, WP 136 (20 June 2007): 11. See also the WP29 opinion on device fingerprinting (profiling on the basis of the devices used to access

webpages), where the device fingerprint is also considered personal data. See Article 29 Data Protection Working Party, Opinion 9/14 on the application of Directive 2002/58/EC to device fingerprinting, WP 224 (25 November 2014): 4.

[28] See also Steppe, 'Online price discrimination and personal data', 774. See also: Frederik J. Zuiderveen Borgesius, 'Singling out people without knowing their name – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation', *Computer Law & Security Review* 32 (2016): 262.

[29] Court of Justice of the European Union, Judgment of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779, paras. 44-49.

[30] See also Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 358. The wide scope of the concept of personal data has been criticised by Purtova, arguing that it will soon become impossible to delineate personal data from non-personal data. In her words, 'European data protection law is facing a risk of becoming "the law of everything"'. See Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology* 10 (2018): 41.

[31] Wim Schreurs, Mireille Hildebrandt, Els Kindt, and Michaël Vanfleteren, 'Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector', in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Serge Gutwirth and Mireille Hildebrandt (Springer, 2008), 248-249

[32] Keystroke dynamics are the unique rhythm generated by a person typing into a computer keyboard. As long as those are not linked to another personal dataset that would render the person identifiable, it is theoretically possible to build anonymous profiles linked to a certain keystroke. See Angelos Yannopoulos, Vassiliki Andronikou, and Theodora Varvarigou, 'Behavioural Biometric Profiling and Ambient Intelligence', in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Serge Gutwirth and Mireille Hildebrandt (Springer, 2008), 95.

[33] For a definition of 'profiling' from a data protection perspective, see the definition in Art. 4(4) GDPR.

[34] See also Steppe, 'Online price discrimination and personal data', 783.

[35] Simone van der Hof and Corien Prins, 'Personalisation and its Influence on Identifies, Behaviour and Social Values', in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Serge Gutwirth and Mireille Hildebrandt (Springer, 2008), 114.

[36] See also the similar analysis by Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 356 and Steppe, 'Online price discrimination and personal data', 773-776.

[37] See Art. 2(2)(a) GDPR. For details on how to analyse whether or not a controller or processor has an establishment within the EU, see: Court of Justice of the European Union, Judgment of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, EU:C:2014:317, paras 55-60.

[38] See Art. 3(2) GDPR. For a discussion of the advantages and pitfalls of this extended territorial applicability of the GDPR, see: Paul de Hert and Michal Czerniaeski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context', *IDPL* 6(3).

[39] The European Parliament has also concluded that data protection rules are applicable to algorithms, precisely because of the risk of discrimination. See: European Parliament, Fundamental rights implications of big data, point 5.

[40] Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 358.

[41] This can be achieved with the right to object of Article 21 GDPR, that is however limited to some forms of processing, and Article 17 GDPR, that gives a right to erasure or 'to be forgotten' in some instances. Both only apply once processing has already taken place.

[42] Gloria Gonzaléz Fuster, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *IDP* 19 (October 2014): 101.

[43] This was clarified by the CJEU in Court of Justice of the European Union, Judgment of 5 May 2011, *Deutsche Telekom AG v Bundesrepublik Deutschland*, C-543/09, EU:C:2011:279, paras 61-65.

[44] Steppe, 'Online price discrimination and personal data', 780. See also Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217 (9 April 2014): 26.

[45] Explained for credit scores in Citroen and Pasquale, 'The scored society', 17-18. See also for the European context: Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation', *IDPL* 7 (2017): 244. The usefulness of informing data subjects about the logics of algorithms was questioned by Wachter et al., stating that an average person might lack the capability to understand even a simple technological representation of the logic involved in an algorithm, due to its high complexity and necessary pre-knowledge. See Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *IDPL* 7 (2017): 98-99.

[46] Tal Zarsky, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency in Automated and Opaque Decision-making', *Science, Technology, and Human Values* 41 (2016): 122.

[47] Michael Veale and Lilian Edwards, 'Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling', *Computer Law & Security Review* 34 (2018): 403.

[48] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness', *CiTiP Working Paper* 29 (2017): 38.

[49] See European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), *Handbook on European Non-Discrimination Law: 2018 Edition* (Luxemburg: Publication Office of the European Union, 2018), 133–39; Julie Ringelheim, 'The Prohibition of Racial and Ethnic Discrimination in Access to Services under EU Law', *European Anti-Discrimination Law Review* 10 (2010): 11–18.

[50] European Union, Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373 (21 December 2004), Recital 13.

[51] See, for instance, European Union, Council Directive 2004/113/EC, art. 2.

[52] European Union, Council Directive 2004/113/EC, art. 3; European Union, Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180 (19 July 2000), art. 3.

[53] European Union, Council Directive 2004/113/EC, art. 5.

[54] Court of Justice of the European Union, Judgment of 1 March 2011, *Association Belge des Consommateurs Test-Achats and Others*, C-236/09, EU:C:2011:100, paras. 30–34.

[55] European Union, Council Directive 2000/43/EC, art. 3.1.(h).

[56] Court of Justice of the European Union, Opinion of Advocate General Kokott delivered on 30 September 2010, *Association Belge des Consommateurs Test-Achats and Others*, C-236/09, EU:C:2010:564, para. 49.

[57] This analysis is confirmed by Schermer starting from a data protection angle. See: Bart Schermer, 'Risks of Profiling and the Limits of Data Protection Law, ' in in *Discrimination & Privacy in the Information Society*, edited by Bart Custers, Toon Calders, Tal Zarsky, and Bart Schermer (Springer, 2013), 139.

[58] These three grounds are included in French anti-discrimination law. See *Loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations* [Law No. 2008-496 of 27 May 2008, containing diverse provisions transposing EU law in the domain of non-discrimination], JORF n°0123 (28 May 2008).

[59] These nineteen criteria are: presumed race, skin colour, nationality, ancestry (Jewish origin), national or ethnic origin, gender, disability, philosophical or religious beliefs, sexual orientation, age, wealth (in other words, financial resources), civil status, political beliefs, trade union membership, health status, physical of genetic characteristics, birth, social background, and language. See *Loi du 10 Mai 2007 tendant à lutter contre certaines formes de discrimination / Wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie* [Law of 10 May 2007, seeking to combat certain forms of discrimination], M.B. / B.S. 30 mai/mei 2007.

[60] See Koops, who argues that 'data protection may be the sister of privacy but she is the twin of equal treatment', in Bert-Jaap Koops, 'Reply: Some Reflections on Profiling, Power Shifts and Protection Paradigms', in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Serge Gutwirth and Mireille Hildebrandt (Springer, 2008), 335

[61] From here on, the terms 'special categories of data' and 'sensitive data' will be used interchangeably.

[62] See Art. 8(2) CFREU ('such data must be processed *fairly* for specified purposes') and Art. 5(1)(a) GDPR.

[63] Veale and Edwards, 'Clarity', 403.

[64] Unfairness is thus a risk of data processing which does not follow the data protection principles. See Veale and Binns, 'Fairer machine learning in the real world', 1.

[65] Clifford and Ausloos, 'Data Protection and the Role of Fairness', 13.

[66] See Raphaël Gellert, Katja DeVries, Paul de Hert, and Serge Gutwirth, 'A Comparative Analysis of Anti-Discrimination and Data Protection Legislations', in *Discrimination & Privacy in the Information Society*, edited by Bart Custers, Toon Calders, Tal Zarsky, and Bart Schermer (Springer, 2013), 68-70

[67] Clifford and Ausloos, 'Data Protection and the Role of Fairness', 15.

[68] The case *Association Belge des Consommateurs Test-Achats and Others* would have also offered the opportunity to analyse from a data protection angle the practice of insurance companies collecting all kinds of personal data for profiling, but the CJEU based its decision solely on anti-discrimination law and did not mention data protection concerns. See on this point also: Gellert et al, 'A Comparative Analysis', 80.

[69] See Court of Justice of the European Union, Judgment of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, C-524/06, EU:C:2008:724.

[70] *Huber*, C-524/06, para 66. For a critical analysis of this approach see: Gellert et al, 'A Comparative Analysis', 76-79.

[71] Art. 8(1) DPD and Art. 9(1) GDPR.

[72] David Kampert, 'Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten', in *Europäische Datenschutzgrundverordnung*, edited by Gernot Sydow (Baden-Baden: Nomos, 2017), 391.

[73] Mireille Hildebrandt, 'Profiling and the Identity of the European Citizen', in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Serge Gutwirth and Mireille Hildebrandt (Springer, 2008), 321.

[74] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, WP 171 (22 June 2010): 19.

[75] Kampert, 'Artikel 9', 394.

[76] According to the Handbook 'European non-discrimination law' the protected grounds include: sex, gender identity, sexual orientation, disability, age, race, ethnicity, colour and membership of a national minority, nationality or national origin, religion or belief or political or other opinion, language, social origin, birth, and property. See FRA and CoE, *Handbook*, 155-160. Note however, that under the EU anti-discrimination directives, these grounds are reduced to: sex, racial or ethnic origin, age, disability, religion or belief, and sexual orientation. See FRA and CoE, 'Handbook', 160.

[77] Zliobate and Custers, 'Using sensitive personal data', 187.

[78] Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 361. Similar for behavioural advertising under the DPD: See WP29, 'Opinion 2/2010', 20.

[79] Kampert, 'Artikel 9', 395.

[80] Art. 9(2)(a) GDPR.

[81] Frederik J Zuiderveen Borgesius, Sanne Kruikemeier, Sophie C Boerman and Natali Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *EDPL* 3 (2017): 6.

[82] Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 359-360.

[83] It might be, however, risky to align sensitive data and prohibited grounds. As Gellert et al. argue, adding for instance gender and age as sensitive data would mean including two of the most processed personal data items. Applying the stricter standard for sensitive data to them could be then seen as disproportionate. See Gellert et al, 'A Comparative Analysis', 89.

[84] See also: Wachter et al., 'Why a Right to Explanation', 81.

[85] The ambiguity of the formulation of Art. 22 GDPR has led to an intense scholarly debate around what Art. 22 means and entails in practice. See Wachter et al., 'Why a Right to Explanation'; Veale and Edwards, 'Clarity', 400; Malgieri and Commandé, 'Why a Right', 243; Andrew D Selbst and Julia Powles, 'Meaningful information and the right to explanation', *International Data Privacy Law* 4 (2017); Marcus Helfrich, 'Artikel 22 Automatisierte Entscheidungen

im Einzelfall einschließlich Profiling', in *Europäische Datenschutzgrundverordnung*, edited by Gernot Sydow (Baden-Baden: Nomos, 2017), 573. In addition, the WP29 provided some guidance, which is however non-binding. See Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01 (last revised and adopted on 6 February 2018): 19.

[86] Wachter et al., 'Why a Right to Explanation', 94-96.

[87] Wachter et al., 95.

[88] WP29, Guidelines, 19.

[89] For Veale and Edwards the guidance of the WP29 even borders on 'unauthorised law-making', showing that the wording of Article 22 GDPR is just too ambiguous to make such a call. See: Veale and Edwards, 'Clarity', 400.

[90] Art. 22(1) GDPR.

[91] As is explained by Wachter et al. such an interpretation for example prevails in Germany. See Wachter et al., 'Why a Right to Explanation, ' 92.

[92] Paul Voigt and Axel von dem Bussche, 'Rights of Data Subjects', in The EU General Data Protection Regulation, edited by Paul Voigt and Axel von dem Bussche (Cham: Springer, 2017), 181.

[93] WP29, Guidance, 19-20.

[94] Steppe, 'Online price discrimination and personal data', 783; Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 361.

[95] Malgieri and Commandé, 'Why a Right', 243.

[96] WP29, Guidelines, 21-22.

[97] See Helfrich, 'Artikel 22', 573. See also WP29, Guidance, 19.

[98] Art. 22(4) GDPR.

[99] Malgieri and Commandé, 'Why a Right', 246.

[100] This alignment seems to be much more successful in the context of the Law Enforcement Directive, regulating processing of personal data in a law enforcement context, where Article 11(3) prohibits profiling resulting in discrimination based on sensitive data with no exceptions. Such a strong stance would have also been welcome in the GDPR. See: European Union, Directive (EU) 2016/680.

[101] Zarsky, 'The Trouble with Algorithmic Decisions', 127.

[102] Zarsky, 'Understanding Discrimination in the Scored Society', 1379. See also Zarsky, 'The Trouble with Algorithmic Decisions', 129.

[103] Malgieri and Commandé, 'Why a Right', 246.

[104] See the exact same wording of Arts. 13(2)(f) and 14(2)(g) GDPR. See also: Malgieri and Commandé, 'Why a Right', 246.

[105] See the detailed assessment of Zuiderveen Borgesius and Poort, 'Online Price Discrimination and EU Data Privacy Law', 361-363. See also, for examples regarding automated decision-making, Voigt and von dem Bussche, 'Rights of Data Subjects', 181.

[106] The high volatility of US stock markets in 2018 has led commentators to argue that algorithms are influenced by external events in an unforeseeable manner, and that they overall resort to more information than previously assumed, including potential personal information. More research on this subject is needed, however. See, for illustration, the news articles by Paul Farrell, 'Are algorithms ruling our investment choices?', *Barrons* (7 December 2018), available at https://www.barrons.com/articles/are-algorithms-ruling-our-investment-choices-1544230800; and Silvia Amaro, 'Sell-offs could be down to machines that control 80% of the US stock market, fund manager says', *CNBC* (5 December 2018), available at https://www.cnbc.com/2018/12/05/sell-offs-could-be-down-to-machines-that-control-80percent-of-us-stocks-fund-manager-says.html.

[107] Voigt and von dem Bussche, 'Rights of Data Subjects', 150.

[108] Malgieri and Commandé, 'Why a Right', 247.

[109] See opposing views of Malgieri and Commandé, 'Why a Right', 245; Wachter et al., 'Why a Right to Explanation,' 84; WP29, Guidance, 19; Veale and Edwards, 'Clarity', 399.

[110] See the example of the algorithm used by the Austrian employment agency (AMS), which was supposed to calculate the chances of each individual to re-enter the job market. Individuals were categorised as not likely, likely or highly likely to re-enter the job market, and resources were allocated according to this categorisation. The company responsible for developing the algorithm published a concept paper outlining its workings, clearly showing that being female, having children, or being over a certain age all counted negatively towards the score. Critics argue that the system discriminates on the basis of gender and age. For our purposes, the fact that there was a concept paper helped determine potential discrimination. Such minimum information already proved useful, even though this was not a case of price discrimination. See Jürgen Holl, Günter Kernbeiß, Michael Wagner-Pinter, 'Das AMS-Arbeitsmarkt-chancen-Modell – Dokumentation zur Methode,' (Oktober 2018), available at http://www.forschungsnetzwerk.at/downloadpub/arbeitsmarktchancen_methode_%20dokumentation.pdf.
Futurezone, 'Der AMS-Algorithmus ist ein "Paradebeispiel für Diskriminierung",' (17 October 2018), available at https://futurezone.at/netzpolitik/der-ams-algorithmus-ist-ein-paradebeispiel-fuer-diskriminierung/400147421.

[111] See also Schermer, 'Risks of Profiling', 145.

[112] See Robert G. Schwemm and Jeffrey L. Taren, 'Discretionary Pricing, Mortgage Discrimination, and the Fair Housing Act', *Harvard Civil Rights-Civil Liberties Law Review* 45 (2010): 375–433; Cassandra Jones Havard, ''On the Take': The Black Box of Credit Scoring and Mortgage Discrimination', *Public Interest Law Journal* 20 (2011): 241–287; Andra C. Ghent, Rubén Hernández-Murillo, and Michael T. Owyang, 'Differences in Subprime Loan Pricing across Races and Neighborhoods', *Regional Science and Urban Economics* 48 (2014): 199–215; Manuel B. Aalbers, *Place, Exclusion and Mortgage Markets* (Chichester and Malden, MA: Wiley-Blackwell, 2011).

[113] See Aalbers, *Place, Exclusion and Mortgage Markets*; Manuel B Aalbers, 'Place-Based Social Exclusion: Redlining in the Netherlands', *Area* 37, no. 1 (2005): 100–109; Luis Diaz-Serrano and Josep M. Raya, 'Mortgages, Immigrants and Discrimination: An Analysis of the Interest Rates in Spain', *Regional Science and Urban Economics* 45 (2014): 22–32; Davide Secchi and Raffaello Seri, 'Experienced Discrimination in Home Mortgage Lending: A Case of Hospital Employees in Northern Italy', *Business & Society* 56, no. 7 (2015): 1068–1104.

[114] Court of Justice of the European Union, Judgment of 16 July 2015, *CHEZ Razpredelenie Bulgaria*, C-83/14, EU:C:2015:480, para. 59.

[115] Zarsky, 'Understanding Discrimination in the Scored Society', 1395. See also: Kate Crawford and Jason Schultz, 'Big data and due process: Towards a framework to redress predictive privacy harms', *Boston College Law Review* 55 (2014):94.

[116] European Data Protection Supervisor, Opinion 3/2018 on online manipulation and personal data (19 March 2018): 8.

[117] See Court of Justice of the European Union, Judgment of 6 November 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, paras. 50-51, where the Court considered the publication of the information that a person had a broken leg a publication of health data, and therefore sensitive data. See, more recently, Court of Justice of the European Union, Opinion of 26 July 2017, *Opinion 1/15*, EU:C:2016:656, paras. 164-167, where the Court was asked to assess the PNR transfer agreement with Canada and found incompatibilities with the fundamental rights of Arts. 7 and 8 of the Charter of Fundamental Rights of the EU, *inter alia* because the agreement potentially allowed the transfer of sensitive data in the form of information about special service information or requests (e.g. food preferences, whether a wheelchair is needed at the airport, etc.) without appropriate safeguards.

[118] EDPS, Opinion 3/2018, 8.

[119] The evidentiary issues are explained e.g. in Pedreschi et al. See: Dino Pedreschi, Salvatore Ruggieri and Franco Turini, 'The Discovery of Discrimination', in *Discrimination & Privacy in the Information Society*, edited by Bart Custers, Toon Calders, Tal Zarsky, and Bart Schermer (Springer, 2013), 100.

[120] Explained as the 'privacy paradox' in Frederik Zuiderveen Borgesius, Sanne Kruikemeier, Sophie C Boerman and Natali Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *EDPL* 3 (2017): 6.

[121] An explanation of the different conditions for consent in EU data protection law can be found in: Frederik Zuiderveen Borgesius, 'Personal data processing for behavioural targeting: which legal basis?' *IDPL* 5(3) (2015): 167. See also: Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, WP 259 rev.01 (revised and adopted 10 April 2018).

[122] See Veale and Binns, 'Fairer machine learning in the real world'.

[123] Such a conclusion can be made relying on the insights provided by behavioural economics, which state that individuals are generally loss-averse. Perhaps by framing data protection violations as a loss in the sense of potential discrimination, loss-aversion would make data subjects more alert. See: Christine Jolls, Cass R. Sunstein and Richard Thaler, 'A Behavioral Approach to Law and Economics', *Stanford Law Review* 50 (1998): 1483-1484.

[124] See especially Zliobate and Custers, 'Using sensitive personal data'.

[125] Zarsky, 'Understanding Discrimination in the Scored Society',1403.

[126] See Julie Ringelheim and Olivier De Schutter, *Ethnic Monitoring: The Processing of Racial and Ethnic Data in Anti-Discrimination Policies: Reconciling the Promotion of Equality with Privacy Rights*, Collection du Centre des droits de l'homme de l'Université catholique de Louvain 6 (Brussels: Bruylant, 2010).

[127] Art. 9(2)(g) and (j).

[128] Kampert, 'Artikel 9', 400.

[129] See Veale and Binns, 'Fairer machine learning in the real world', for suggestions on alternatives to using sensitive data.

[130] See Gellert et al, 'A Comparative Analysis', 89.

[131] See Akiva A. Miller, 'What Do We Worry about When We Worry about Price Discrimination? The Law and Ethics of Using Personal Information for Pricing', *Journal of Technology Law and Policy* 19 (2014): 96.

[132] Hacker reaches a similar conclusion examining algorithms under EU anti-discrimination and data protection law from a general perspective. See Philipp Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination in EU Law', *Common Market Law Review* 55 (2018): 1184.