

Opening the Black Box of Technology: The Place of Fundamental Rights
Brussels, 18 May 2018

**Data Protection and Discrimination
in the Age of Pricing Algorithms**

LAURA DRECHSLER

laura.drechsler@vub.be

PhD Researcher, Brussels Privacy Hub, LSTS, Vrije Universiteit Brussel (Belgium)

JUAN CARLOS BENITO SÁNCHEZ

juan.benito@uclouvain.be

PhD Researcher (F.R.S.-FNRS FRESH), Centre de philosophie du droit,
Université catholique de Louvain (Belgium)

1. Introduction

At a time where companies process massive amounts of personal data enabling them to generate complex profiles of consumers, the question of how the fundamental rights of data protection and nondiscrimination in the European Union (EU) can still guard individuals against abuses arises with special impetus. Although the issue of “price discrimination” via algorithms has been analysed from the standpoint of how these algorithms are designed and in relation to the General Data Protection Regulation (GDPR),¹ an enquiry into how antidiscrimination law specifically interacts with data protection law remains crucial to understand how individuals are protected in their access to goods and services, especially in the context of pricing algorithms.

The term “price discrimination” can have different meanings. From an economic point of view the concept describes the process of matching customers with the price they are willing to pay.² In other words, it is pricing a product in a way that takes the personal attributes of the potential customer into account.³ This view also considers other elements like offering specific discounts or vouchers to certain individuals or groups as part of pricing discrimination. From that perspective, price discrimination is desirable insofar as it creates a better match between offer and demand and according to some authors this even increases the total welfare. Other authors limit this to certain situations.⁴ From a data protection and an antidiscrimination law point of view, price discrimination means that the price of a product or a service differs depending on the personal information of users which the supplier of the product or service has available.⁵

¹ European Union, Regulation (EU) 2016/679 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 96/46/EC (General Data Protection Regulation), OJ L 119 (4 May 2016).

² Richard Steppe, “Online price discrimination and personal data: A General Data Protection Regulation perspective,” *Computer Law & Security Review* 33 (2017): 769.

³ 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.

⁴ It has 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.

⁵ Zuiderveen Borgesius and Poort, “Online,” 348.

In this paper, we would have an understanding of price discrimination going more into the direction of the latter definition. By price in this context we do not only mean the retail price in a sale context, but more generally any monetary cost that individuals have to bear to obtain a good or service, e.g. including insurance premiums, loan interest rates etc. For price discrimination, we will focus on the price determined by an algorithm for a certain individual and not on other elements like vouchers or discounts based on price sensitivity (for example, to students or the elderly). Thus, price discrimination for this paper signifies using information revealing individual or group characteristics in order to determine the monetary cost to assign to them.

The paper starts by discussing in section 2 in how far data protection law can play a role when assessing pricing algorithms. This includes an analysis of whether companies are allowed to process sensitive personal data, since those are particularly sensitive in relation to fundamental rights and freedoms and coincide or overlap for the most part with the protected grounds of EU antidiscrimination law. Section 3 recalls that collecting and using certain data to determine an individual's ability to access goods and services may circumvent the prohibition to discriminate contained in the EU antidiscrimination directives and in EU fundamental rights law. Bringing our analysis further, section 4 focuses on commonalities and differences of EU data protection and antidiscrimination law when dealing with price discrimination through algorithms. Reflecting on the three previous sections, Section 5 concludes our paper, bundling our arguments together and considering the broader implications of the interaction between these two fields of law through the example of pricing algorithms.

2. Data Protection and pricing algorithms

2. 1. Pricing algorithms and the applicability of EU data protection law

Algorithms present the technological opportunity to track and monitor individuals. This is enabled by a large-scale collection, aggregation and analysis of personal data,⁶ or in other words the use of “Big Data.”⁷ Pricing algorithms use these techniques to try to achieve a better matching of customer and price from the perspective of a commercial entity, in the sense that a customer is “scored” in order to be shown the “right” price depending on his or her profile. Pricing algorithms can be applied in retail (e.g. Amazon experimented with pricing algorithms in 2000),⁸ insurance rates⁹ (e.g. for car insurances) and mortgage and credit applications (an algorithm might decide which rate to show individuals initially).¹⁰ Their use can result in matching customers with the maximum price they are willing to pay (economic view of price

⁶ Paul De Hert, Serge Gutwirth, Anna Moscibroda, David Wright and Gloria González Fuster, “Legal safeguards for privacy and data protection in ambient intelligence,” *Pers Ubiquit Comput* 13 (2009): 436.

⁷ 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 collation, processing, analysis and use of vast exploitable datasets of unstructured and structured digital information.”

⁸ Mark Ward, “Amazon’s old customers ‘pay more’,” *BBC News*, September 8, 2000, <http://news.bbc.co.uk/2/hi/business/914691.stm>.

⁹ 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,” 484-484.

¹⁰ 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/?__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>.

discrimination) but also in targeting of a specific type of customer while excluding those not of that profile. Such profiled targeting can lead to discriminatory outcomes and hence to price discrimination in the sense of this paper, especially if it leads to higher prices or premiums for individuals based on prohibited grounds.¹¹ While it is sometimes argued that assessing individuals via algorithms actually provides less discriminatory results, as un-biased machines are less prejudiced,¹² it must be remembered, that algorithms are not neutral as they are programmed by people for people.¹³ Additionally the databases sourcing these algorithms can contain flawed information entered by biased individuals.¹⁴ The use of pricing algorithms for price discrimination therefore does not alleviate concerns that they might include prohibited grounds under EU antidiscrimination law as variables potentially hidden in the “black box” of the algorithm.¹⁵ Rather, through the pervasive use of large personal data sets, it raises the risks for the individuals, who might also be affected in their fundamental right to data protection.¹⁶

Within the EU several data protection instruments ensure that in principle processing of personal data (also by algorithms) must be fair, lawful and transparent. These instruments are the Data Protection Directive (DPD, still in force until 25 May 2018),¹⁷ the GDPR (applicable from 25 May 2018), and the e-Privacy Directive (EPD).¹⁸ To assess whether these instruments have any relevance for questions concerning pricing algorithms and discrimination, it is first necessary to test the applicability of EU protection law in general. The two key concepts for such applicability are “personal data” and “processing of personal data.” The concept of “personal data” of EU data protection law was firstly defined in Article 2 (a) DPD¹⁹ and has been clarified with Article 4 (1) GDPR.²⁰ It includes any information with which someone can

¹¹ 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 is establishing a link between the U.S. subprime mortgage crisis and credit-scoring based on race. See also Tal Z. Tarsky, “Understanding Discrimination in the Scored Society,” *Wash. L. Rev.* 89 (2014): 1384.

¹² Danielle Keats Citron and Frank Pasquale, “The scored society: Due process for automated predictions,” *Wash. L. Rev.* 89 (2014): 4-5.

¹³ 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.

¹⁴ Citroen and Pasquale, “Scored Society,” 13-14. Tarsky, “Understanding,” 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.

¹⁵ See Citroen and Pasquale, “Scored Society,” 24. See also using the example of U.S. credit scoring, Havard, “Black Box,” 250.

¹⁶ Belleflame and Vergote even suggest that data subjects that are taking privacy protecting measures are charged higher prices for being unidentified, see Paul Belleflame and Wouter Vergote, “Monopoly price discrimination and privacy: The hidden cost of hiding,” *Economics Letters* 149 (2016): 141-144.

¹⁷ 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 paper will include 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.

¹⁸ Directive 2002/58 of 12 July 2002 concerning the processing of 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).

¹⁹ Art. (2) (a) DPD: “‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;.”

²⁰ Art. 4 (1) GDPR: “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;.”

either be directly identified or becomes identifiable. An important role in this context is played by “identifiers” which are information that renders a person identifiable. According to the Working Party Article 29 (WP29) information can relate to a person and make him or her identifiable, if the use of the personal data would have an effect on the concerned person’s rights and freedoms.²¹

In general, identifiability is context-dependent.²² In *Breyer* the Court of Justice of the European Union (CJEU) considered dynamic IP addresses personal data, as for the concrete controller in that case (an online media service provider) it would have been possible to identify the person behind it.²³ Thus, the concept of personal data has principally a very broad scope.²⁴ Considering, the fact that pricing algorithm will consider such information as IP-address, location, device, or customer profile, it seems safe to assume that they usually use personal data to arrive at their pricing result.²⁵ Hence, the first condition for applicability of EU data protection law seems to be fulfilled.

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, and therefore also the second element for applicability of data protection law is fulfilled.²⁶

The fact that EU data protection law will principally apply to pricing algorithms, does not mean that per se EU data protection law prohibits such algorithms.²⁷ In general, EU data protection law does not provide an *ex ante* choice to individuals on whether or not they want their data to be processed (in some cases data subject rights give the possibility to object to processing or delete a result of processing *ex post*). The only exception is the choice whether or not to consent in cases, where the lawful basis for the processing is individual consent.²⁸ However, even in consent situations, the individual cannot choose who is allowed to process their personal data if the processing is covered by the original purpose of collection.²⁹ The applicability of EU data protection law on pricing algorithms results however in the applicability of the EU data protection principles, now neatly enumerated in Article 5 (1) (a) GDPR.³⁰ These principles

²¹ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136 (20 June 2007): 11.

²² See also Steppe, “Online,” 774.

²³ Court of Justice of the European Union, Judgment of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland* C-582/14, ECLI:EU:C:2016:779, paras 44-49.

²⁴ See also Zuiderveen Borgesius and Poort, “Online,” 358.

²⁵ See also Steppe, “Online,” 783.

²⁶ See also the similar analysis by Zuiderveen Borgesius and Poort, “Online,” 356 and Steppe, “Online,” 773-776.

²⁷ Zuiderveen Borgesius and Poort, “Online,” 358.

²⁸ Gloria González Fuster, “How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection,” *IDP* 19 (October 2014): 101.

²⁹ 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, ECLI:EU:C:2011:279, paras 61-65.

³⁰ Art. 5 (1) (a) GDPR: “Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (...) (‘purpose limitation’); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are

include *inter alia* the requirements of transparency and lawfulness, which are especially relevant for the use of algorithms and concerns about discrimination. The principle of transparency is important for pricing algorithms, as the data subject must not be surprised by its application.³¹ Transparency for some includes the notion that data subjects must be in a position to understand how their actions influence the result of the algorithm. In other words, they must understand the basic logic behind the workings of the algorithm.³² In any case, the principle of transparency demands that data subjects are aware of the personal data being collected about them and can correct the data that are inaccurate.³³ The principle of lawfulness requires that data processing can only take place when one of the legitimate grounds of Article 6(1) or Article 9(2) GDPR applies. Article 6(1) lists the legitimate grounds for processing for non-sensitive personal data. According to Zuiderveen Borgesius and Poort the only legitimate basis for the use of pricing algorithms is consent of the data subject concerned, as none of the other grounds is applicable in the specific context of pricing algorithms.³⁴ Article 9(2) GDPR lists legitimate grounds for the processing of sensitive data, which are special categories of data whose processing is principally prohibited.³⁵ This article will focus on the potential processing of sensitive data by pricing algorithms, since such processing shows the most correlations with EU antidiscrimination law.³⁶

2. 2. Processing of sensitive data

As mentioned above, the processing of sensitive data is principally prohibited in EU data protection law.³⁷ The protected categories for sensitive personal data according to Article 9 (1) GDPR³⁸ are similar to the protected grounds of EU antidiscrimination law,³⁹ though small

processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (...) ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

³¹ Steppe, "Online," 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.

³² Explained for credit scores in Citroen and Pasquale, "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.

³³ Tal Tarsky, "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.

³⁴ Zuiderveen Borgesius and Poort, "Online," 360.

³⁵ See Art. 9 (1) GDPR. The DPD and the GDPR term "sensitive data" as "special categories of data." Whenever the term "sensitive data" is being used subsequently, the meaning of "special categories of data" as used by the DPD and GDPR is implied.

³⁶ For an extensive analysis of processing of non-sensitive data by pricing algorithms, see Zuiderveen Borgesius and Poort, "Online," and Steppe, "Online,."

³⁷ Art. 8 (1) DPD and Art. 9 (1) GDPR.

³⁸ Art. 9(1) GDPR: "*Processing of personal 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 shall be prohibited.*"

³⁹ According to 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, language, social origin, birth and property or political or other opinion. 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), 155-160. Note however, that under the EU nondiscrimination 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.

differences exist,⁴⁰ 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. Sensitive data are considered especially worthy of protection due to their close connection to various fundamental rights.⁴¹ 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 the individual.⁴² The use of sensitive data for pricing algorithms can be considered a similar serious risk from an EU data protection perspective.

A particular question in relation to sensitive data is how to handle proxies for such data. Through the sheer amount of personal data algorithms have at their disposal, proxies are more likely to be found and used.⁴³ This according to the European Data Protection Supervisor (EDPS) leads to the risk that “*highly sensitive data (...) can be predicted from seemingly non-sensitive information, such as (...) key stroke dynamics.*”⁴⁴ So far, the CJEU has been very strict about sensitive data and applied the special regimes also to cases where proxies have been used⁴⁵, allowing for the assessment that at least clear proxies for sensitive are not sufficient to avoid the special protection of EU data protection law for sensitive data.

Just as non-sensitive personal data, sensitive data require a specific legitimate basis to be processed. These legitimate bases of Article 9(2) GDPR are in generally more strict compared to the ones enlisted in Article 6(1) GDPR, though overlaps can occur.⁴⁶ According to Zuiderveen Borgesius and Poort, there is only one realistically possible legitimate basis for the processing of sensitive data by a pricing algorithm, namely explicit consent by the data subject.⁴⁷ 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.⁴⁸ In addition, the GDPR provides the opportunity for Member States and other Union acts to exclude certain forms of sensitive data processing from this legal basis, meaning that they can legislate that in certain instances it is not possible to consent to the processing of sensitive data at all.⁴⁹ Processing on the basis of Article 9 (2) (e) “*processing relates to personal data which are manifestly made public by the data subject*” would probably not apply in case of pricing

⁴⁰ Zliobate and Custers, “Using,” 187.

⁴¹ David Kampert, “Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten,” in *Europäische Datenschutzgrundverordnung*, edited by Gernot Sydow (Baden-Baden: Nomos, 2017), 391.

⁴² Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, WP 171 (22 June 2010): 19.

⁴³ Tarsky, “Understanding,” 1395.

⁴⁴ European Data Protection Supervisor, Opinion 3/2018 on online manipulation and personal data (19 March 2018): 8.

⁴⁵ See Court of Justice of the European Union, Judgment of 6 November 2003, *Bodil Lindqvist* C-101/01, ECLI: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 recent, Court of Justice of the European Union, Opinion of 26 July 2017, *Opinion 1/15*, ECLI: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 Charter of Fundamental Rights of the EU (CFREU), *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) without appropriate safeguards.

⁴⁶ Kampert, “Artikel 9,” 394.

⁴⁷ Zuiderveen Borgesius and Poort, “Online,” 361. Similar for behavioural advertising under the DPD, WP29, “Opinion 2/2010,” 20.

⁴⁸ Kampert, “Artikel 9,” 395.

⁴⁹ Art. 9 (2) (a) GDPR.

algorithms, as public information is only such that has been actively and willingly made public by the individual.⁵⁰ Inferences that are drawn from various sources from the internet cannot be considered such information. As Zuiderveen Borgesius and Poort note, due to the unpopularity of pricing algorithms their reliance on consent as a legitimate base for the processing of sensitive data seems difficult in practice.⁵¹

As a final point in this section it is important to note, that it is sometimes argued that the detection of discriminatory bias in algorithms can only occur via the processing of sensitive data.⁵² Especially Tarsky highlights that algorithms can only be tested for some sorts of discrimination by using sensitive data.⁵³ Antidiscrimination law scholars have similarly shown that the availability of such data is key to develop nondiscriminatory policies and practices.⁵⁴ 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.⁵⁵ 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.⁵⁶ This legitimate base is however only suitable for individuals preparing a concrete court action, and not for generally testing potential discrimination via a pricing algorithm. None of the mentioned legal bases, seems however obvious, and more reflection on this question from an EU data protection perspective is needed.⁵⁷

2.3. Remedies provided by EU data protection law

Concerns surrounding the use of pricing algorithms can often be linked to problems of transparency,⁵⁸ especially concerning the individual’s right to have a voice in data processing about him or her, which in EU data protection law is ensured by data subject rights.⁵⁹ An effective application of data subject rights could thus be a potential tool provided by EU data protection law to prevent discrimination via pricing algorithms. Data subject rights of relevance for pricing algorithms are those helping to raise transparency, namely the right to information (Articles 13 and 14 GDPR), the right of access (Article 15 GDPR) and the right not to be subject to automated decision-making (Article 22 GDPR).⁶⁰

⁵⁰ Kampert, “Artikel 9,” 399-400.

⁵¹ Zuiderveen Borgesius and Poort, “Online,” 359-360.

⁵² See especially Zliobate and Custers, “Using,”

⁵³ Tarsky, “Understanding,” 1403.

⁵⁴ 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).

⁵⁵ Art. 9 (2) (g) and (j).

⁵⁶ Kampert, “Artikel 9,” 400.

⁵⁷ See Veale and Binns, “Fairer,” for suggestions on alternatives to using sensitive data.

⁵⁸ Tarsky, “Trouble,” 127.

⁵⁹ Tarsky, “Understanding,” 1379. See also Tarsky, “Trouble,” 129.

⁶⁰ Malgieri and Commandé, “Why,” 246.

The GDPR introduced important clarifications to the right to information of the data subject, which varies depending in whether or not the personal data were collected directly from the data subject.⁶¹ In both instances, the GDPR prescribes that the data subject be informed “*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*.”⁶² This corresponds with the data protection principle of transparency mentioned above and should encompass nearly all pricing algorithm, as they can be considered profiling by automated means.⁶³

The right of access is meant as a tool for data subjects to verify fairness and transparency of data processing concerning them.⁶⁴ Compared to the information rights of the data subject, it is a right to be used *ex post*, so after the processing has occurred.⁶⁵ Requests can be framed specially or more generally concern data processing at a specific controller and must be complied with no later than one month after it was received.⁶⁶ Article 15 (1) GDPR lists under (h) an information obligation with the same wording as Articles 13(2)(f) and 14(2)(g) GDPR, meaning that an access request in the context of an algorithm must be accompanied by information about the workings of an algorithm and possible consequences for the data subject.

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.⁶⁷ The fact that Article 22 GDPR only applies to “*solely automated decision*” could be interpreted as meaning that any type of human intervention renders the provision inapplicable. However, according to Voigt and Von Dem Busche 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.⁶⁸ According to some authors the condition that the automated decision must have “*legal or similar effects*” means, that Article 22 GDPR only applies to pricing algorithms, when the pricing algorithms led to a higher monetary cost for the data subject (hence not to reductions).⁶⁹ As the GDPR does not specify these legal or similar effects, much will depend on interpretation by the CJEU. Due to the economic effect of prices, it seems likely that the provision of Article 22 GDPR will apply to most pricing algorithms. “Price discrimination” is also listed as an example for such effects by Malgieri and Comandé.⁷⁰

Article 22 GDPR has special provisions for the processing of sensitive data. According to Article 22 (4) GDPR this right concerning automated individual decision-making is always

⁶¹ Arts. 13 and 14 GDPR.

⁶² See the exact same wording of Arts. 13(2) (f) and 14(2) (g) GDPR. See also: Malgieri and Commandé, “Why,” 246.

⁶³ See detailed assessment of Zuiderveen Borgesius and Poort, “Online,” 361-363. See also examples for automated decision-making by 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.

⁶⁴ Voigt and von dem Bussche, “Rights,” 150.

⁶⁵ Malgieri and Commandé, “Why,” 247.

⁶⁶ See Art. 12 (3) GDPR. See also Voigt and von dem Bussche, “Rights,” 151.

⁶⁷ Art. 22 (1) GDPR: The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

⁶⁸ Voigt and von dem Bussche, “Rights,” 181.

⁶⁹ Steppe, “Online,” 783. Zuiderveen Borgesius and Poort, “Online,” 361.

⁷⁰ Malgieri and Commandé, “Why,” 243.

applicable if sensitive data are being processed.⁷¹ Article 22 GDPR therefore includes a general prohibition of automated decision-making based on sensitive data.⁷² This prohibition knows only two exceptions, first when the processing of the sensitive data was based on explicit consent according to Article 9 (2) (a) GDPR or second, when the processing was based on a substantial public interest according to Article 9 (2) (g) GDPR. 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 to a pricing algorithm processing sensitive data, the processing can only take place with “*suitable measures*” securing the data subject’s rights and freedoms.⁷³ According to Malgieri and Comandé those measures include at least “*the right to obtain human intervention,*” and “*the right to contest the decision.*”⁷⁴ Malgieri and Comandé also argue that Article 22 GDPR combined with the information rights of Articles 13 and 14 GDPR and the right of access of Article 15 GDPR provide the data subject with a generally applicable “*right to legibility*” about the functionalities of an algorithm and the logic behind an individual decision.⁷⁵ This point is heavily contested by other authors though.⁷⁶

An additional remedy in the context of pricing algorithms is provided by the EPD and its rule on the placement of cookies and other tracking mechanisms. Pricing algorithms rely on cookies to collect the necessary information for building a pricing profile.⁷⁷ The use of so-called “device fingerprinting techniques” can also service profiling purposes, with device fingerprints being personal data according to WP29.⁷⁸ According to Article 5 (3) EPD,⁷⁹ such mechanisms can only be placed with the consent of the data subject.⁸⁰ This rule knows only two exceptions, first when the cookies or fingerprint was solely placed to carry out transmission of a communication, and second, when such placement is necessary to provide an information society service that the data subjects themselves requested.⁸¹ Neither of these exceptions is very likely to apply in case of pricing algorithms as it goes further than a mere communication

⁷¹ Art. 22 (4) GDPR: “*Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.*”

⁷² Marcus Helfrich, “Artikel 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling,” in *Europäische Datenschutzgrundverordnung*, edited by Gernot Sydow (Baden-Baden: Nomos, 2017), 573.

⁷³ Art. 22 (4) GDPR.

⁷⁴ Malgieri and Commandé, “Why,” 246.

⁷⁵ Malgieri and Commandé, “Why,” 245: “*(...) legibility of data and analytics algorithms is a concept able to combine comprehensibility of the functioning of the algorithm (...) with transparency about the commercial use of that algorithm (...) in an effective way.*”

⁷⁶ 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).

⁷⁷ Zuiderveen Borgesius and Poort, “Online,” 352.

⁷⁸ Article 29 Data Protection Working Party, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224 (25 November 2014): 4-6.

⁷⁹ Art. 5(3) EPD: “*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*”

⁸⁰ Zuiderveen Borgesius and Poort, “Online,” 358. See also WP29, “Opinion 2/2010,” 3, and WP29, “Opinion 9/2014,” 8.

⁸¹ WP29, “Opinion 9/2014,” 7.

requests, and does not constitute an information society service,⁸² therefore the consent requirement of the EPD can be an additional safeguard to protect the individual from tracking via algorithm.

2.4. Preliminary conclusions

As this section has indicated, EU data protection law includes safeguards and opens potential venues to address discrimination by pricing algorithms. The safeguards include its specific protection for sensitive data, whose definition largely overlaps with the protected grounds of EU antidiscrimination law, but excludes the important grounds gender and age. The fact that sensitive data can only be processed based on explicit consent which needs to refer to the processing of sensitive data, could put up an important barrier against pricing algorithms using such data. However, consent has proven to be less of an insurmountable barrier in the past, as data subjects tend to consent without reading the details.⁸³ For this reason, data subject rights, which provide remedies to counter-balance opacity, could prove to be an important second safeguard. The rights to information and of access could be used to obtain crucial information in order to prove discrimination, if a data subject is willing to personally engage against a pricing algorithm. Most importantly, Article 22 GDPR includes a general prohibition of automated decision-making without human intervention based on sensitive data. Unfortunately, once again consent is an exception. A similar problem exists for the remedy provided by the EPD, requiring consent for the placing of tracking tools, as also this provision can be avoided by obtaining consent of the data subject. The flaw from a data protection perspective for protecting individuals against discrimination by pricing algorithms hence lays in the heavy reliance of its remedies on consent. Nevertheless, a motivated individual could use data protection tools to uncover discrimination and as Article 80 GDPR introduces the possibility to “*mandate a not-for-profit body, organisation or association*” with the exercise of the rights of the data subject this role could be facilitated by active NGOs and associations.

3. Pricing algorithms and antidiscrimination law

Pricing decisions taken by algorithms can be problematic from an antidiscrimination law perspective. By determining the monetary costs that individuals incur in to obtain a particular good or service—be it in the form of retail prices, insurance premiums, loan interests, or others—, pricing decisions have an impact on the access of individuals and groups to the market. According to antidiscrimination 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.

⁸² According to Art. 1 (1) (b) European Union, Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance), OJ L 241 (17 September 2015), “Information Society service” means “*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.*” It is doubtful whether pricing algorithms would fit that definition.

⁸³ Explained as the “privacy paradox” in 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.

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.⁸⁴ 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.”⁸⁵ This means that a pricing decision taken by an algorithm in the framework of these activities will generally come under the scope of antidiscrimination law, since it concerns goods and services available to the public. This will certainly be the case for the three modalities more closely explored in this paper: online retail stores, insurance, and banking services.

According to antidiscrimination 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).⁸⁶ In other words, in order to comply with antidiscrimination 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 these decisions do not have a disproportionate impact on certain groups without an adequate justification.

For the purposes of this paper, we will focus on direct discrimination as the most immediate type of discrimination likely to emerge from pricing decisions taken by algorithms. 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) used the same legacy web browser on dated computer equipment for which the manufacturer no longer provides security updates, and saw higher prices as a consequence, a case might be made for indirect age discrimination. However, indirect discrimination cases will be less frequent and harder to prove than direct discrimination cases in this context.

At the EU level, discrimination in the access to goods and services is prohibited on the grounds of gender and of racial or ethnic origin.⁸⁷ For instance, if an algorithm establishes higher prices for women than men on account of the user’s gender, this will be considered discriminatory.

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

⁸⁴ See FRA and CoE, “Handbook,” 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.

⁸⁵ 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.

⁸⁶ See, for instance, European Union, Council Directive 2004/113/EC, art. 2.

⁸⁷ 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.

result in differences in individuals' premiums and benefits.”⁸⁸ 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 nondiscrimination enshrined in Articles 21 and 23 of the EU Charter of Fundamental Rights.⁸⁹ Even those contracts which were concluded before the entry into force of the Directive, which were afforded a transitional legal regime, must now comply with this rule. As a result, it is clear that today insurance premiums and benefits cannot be calculated using sex as factor, even if this is just one among other factors.

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.⁹⁰ 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.⁹¹

Pricing algorithms, as established above, affect the ability of individuals and groups to access goods and services. If the monetary cost incurred in 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.

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 the particular vulnerability resulting from their economic situation.⁹² 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.⁹³

⁸⁸ European Union, Council Directive 2004/113/EC, art. 5.

⁸⁹ 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.

⁹⁰ European Union, Council Directive 2000/43/EC, art. 3.1.(h).

⁹¹ Court of Justice of the European Union, 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.

⁹² These three grounds are included in French antidiscrimination 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 nondiscrimination], JORF n°0123 (28 May 2008).

⁹³ 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,

We have discussed until now the situation whereby a merchant (controller) uses sensitive personal data aligned with prohibited discrimination grounds to take pricing decisions via an algorithm. However, what happens if a merchant does not process sensitive personal data, but uses the complex set of information they possess about a particular person to infer this 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. An individual living nearby 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.

As long as a decision is ultimately taken “on the basis of” one of the prohibited grounds, this will constitute (prohibited) direct discrimination. 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.⁹⁴ Similar practices have also been documented in the European context.⁹⁵ 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 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 the decision to reject an applicant or to charge higher interest rates will be considered direct discrimination, since racial or ethnic origin is ultimately being used as the basis to take that decision. 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,

financial resources), civil status, political beliefs, trade union membership, health status, physical or 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.

⁹⁴ 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).

⁹⁵ 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.

which constitutes the factor on the basis of which she considers that she has suffered less favourable treatment or a particular disadvantage.”⁹⁶

If a *prima facie* case is convincingly made in the sense that an algorithm has taken a decision based on these factors, the sharing or shifting of the burden of proof characteristic to antidiscrimination law will apply. In that event, the respondent individual or company must be able to prove that the decision was exclusively founded on objective factors unrelated to any discrimination on any prohibited grounds.⁹⁷ Otherwise, the practice will be found discriminatory.

All in all, it must be emphasised that the key issue here is that goods should be allocated to anyone willing or able to pay their price, and not according to personal circumstances. In other terms, 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.⁹⁸ It follows that antidiscrimination law is indeed concerned with pricing decisions taken by algorithms, insofar as it prohibits discrimination in access to goods and services. Beyond the protection offered by privacy and data protection law, antidiscrimination law adds an extra layer of safeguards, focusing on whether decisions are taken on the basis of prohibited grounds or have a disproportionate impact on certain groups without an adequate justification—thus enhancing and securing important fundamental rights.

4. Commonalities and differences (points to be developed for the final paper)

As it can be seen from the two previous sections, neither EU data protection law nor EU antidiscrimination law alone seem to provide complete protection against pricing algorithms discriminating on the basis of protected grounds. This situation seems unacceptable, considering that both data protection and nondiscrimination are considered fundamental rights in an EU context. Both of these rights call into question the supposed neutrality of certain algorithms, and highlight the fact that flawed information and bias can be found behind certain pricing decisions. This section therefore aims to explore whether using a combination of EU data protection and antidiscrimination approaches could be a way forward and highlights the current limitations to such a combined approach.

A combined approach offers indeed several opportunities. While antidiscrimination law is most fitted to the wrong that occurs when algorithm decisions on pricing are based on protected grounds, as it is precisely this wrong it is meant to address, EU data protection law can offer the transparency tools needed to uncover the discriminatory practice underlying it. Data subject rights such as the right to information and the right of access could play an important role in obtaining evidence establishing that an algorithm’s decision is indeed based on protected grounds. Based on these findings, a claim under EU antidiscrimination law could have higher chances of achieving the high standard of evidence required to prove direct discrimination in the access to goods and services. Additionally, the stricter rules on sensitive data and automated

⁹⁶ Court of Justice of the European Union, Judgment of 16 July 2015, *CHEZ Razpredelenie Bulgaria*, C-83/14, EU:C:2015:480, para. 59.

⁹⁷ See Court of Justice of the European Union, *CHEZ Razpredelenie Bulgaria*, para. 85.

⁹⁸ 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.

decision-making without human intervention could prove important thresholds to keep merchants (controllers) from engaging in such practices in the first place.

An important commonality of EU data protection and antidiscrimination law also lays in their treatment of proxies for “sensitive data” or “protected grounds.” For both, the CJEU has set a strict standard, so that sensitive data and antidiscrimination rules cannot be easily circumvented by the use of proxies. A further development of the arguments for equalising proxies with sensitive data or protected grounds should therefore be undertaken from both legal perspectives and happen aligned to each other.

It would also be of use, if EU antidiscrimination law could outbalance the limitations of the EU data protection law approach and vice-versa. The biggest hindrance to an effective data protection law approach against discrimination via pricing algorithm is the heavy reliance on consent and the “privacy paradox,” that leads to individuals consenting to different kinds of processing without knowing the details, while at the same time being concerned about privacy and data protection. The injury of being potentially discriminated against based on a protected ground could lead to more awareness in individuals and they might therefore pay closer attention. More research into this is needed though.

An important limitation of a combined approach between EU data protection law and antidiscrimination law is the fact that neither gender nor age are considered full sensitive data under EU data protection law (although if either can be linked to health this could change). The protection against discrimination in access to goods or services is especially strong in relation to gender in the EU, therefore its lack of protection as sensitive data is regrettable. While data subject rights such as access and information will also be available for non-sensitive data, the prohibition of Article 22 GDPR for automated decision-making based on sensitive data will not apply.

Finally, for EU antidiscrimination law experts it is clear that the only method for successfully detecting discrimination in pricing algorithms is testing them with the use of sensitive data. For this, the current EU data protection law seems to lack a clear legitimate base justifying the processing, though more research is needed here and it will also depend on the interpretation of the GDPR by the CJEU.

5. Conclusions

For the conclusions we wish to profit from the feedback and comments received during our presentation, especially on the ideas in section 4. We will therefore leave this section for the final version.