EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

The omnibus directive and online price personalization: a mere duty to inform?

SEBASTIÃO BARROS VALE
LL.M in EU law at the College of Europe in Bruges (Belgium)
Lawyer in Portugal

Abstract

As part of the EU's New Deal for Consumers, Directive (EU) 2019/2161 (the Omnibus Directive) enshrines into European law a duty for traders to inform consumers who visit their online stores if the prices they are offered have been tailored based on their personal traits by a pricing algorithm. Although this commercial tactic sounds innovative, the phenomenon of Online Price Personalization (OPP) is not new, as retailers have been reported to embark on such practices since the turn of the millennium. Consumers have expressed feelings of discomfort and outrage towards OPP, even in cases where it could work to their advantage (i.e., leading them to pay a lower price when compared to other consumers). This paper will look to offer a clear definition of OPP, setting it apart from similar practices. It will also elaborate on how consumers should be informed about OPP under the Omnibus Directive and seek to outline the current constraints EU law poses to OPP. While EU anti-discrimination law is briefly analyzed, deeper focus will be dedicated to Privacy & Data Protection Law and the Unfair Commercial Practices Directive (UCPD) as means to protect consumers from OPP, regardless of whether it discriminates against them or not. The paper will try to demonstrate how, in several cases, traders deploying OPP may be misleading consumers for the purposes of Articles 6 and 7 of the UCPD, and how the "average consumer" criterion is unfit to legally assess the fairness of OPP under the UCPD.

Keywords: Online Price Personalization - European Union - New Deal for Consumers - Discrimination - Omnibus Directive - General Data Protection Regulation - Unfair Commercial Practices.

Summary: Introduction – 1. Defining Online Price Personalization (OPP). – 2. The Omnibus Directive: an insufficient shield against OPP. – 3. The EU anti-discrimination framework: limited safeguards and a heavy burden of proof. – 4. EU Privacy and Data Protection law: a big hurdle for OPP. – 5. OPP as an Unfair Commercial Practice? – Conclusions.

List of Abbreviations:

AI = Artificial Intelligence
BEUC = The European Consumer Organization
Council = Council of the European Union
Charter = Charter of Fundamental Rights of the European Union [2000] O.J. C364 1
CJEU = Court of Justice of the European Union
CRD = 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 (Consumer Rights Directive) [2011] OJ L304/64
DPA = Data Protection Authority, as per Article 4(21) GDPR

DPD = Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L281

EC = European Commission

EP = European Parliament

EDPB = European Data Protection Board created under Article 68 of the GDPR

ePrivacy Directive = Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2002] OJ L201

EU = European Union

GDPR = Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing DPD (General Data Protection Regulation) [2016] OJ L119/1

GGSD = 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 (Gender Goods and Services Directive [2004] OJ L373/37

Geo-blocking Regulation = Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC [2018] OJ LI60/1

OECD = Organization for Economic Co-operation and Development

Omnibus Directive = Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7

OPP = online price personalization

RED = Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (Race Equality Directive) [2000] OJ L180

Rome I Regulation = Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations [2008] OJ L177/6

Services Directive = Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [2006] OJ L376/36

TEU = Consolidated Version of the Treaty on European Union [2008] OJ C115/13. Treaty on European Union (Maastricht Treaty) art G5

TFEU = Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326

UCPD = Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22

WP29 = Working Party created under Article 29 of the DPD
WTP = willingness to pay

Introduction.

Imagine you are comparing dog food prices online, on the website where you normally buy it, and notice the retailer was offering a great deal for this normally expensive packet. Then, after logging in with your user credentials, the deal suddenly disappears, as the price for each such packet rises significantly. Does this make you think that you are being asked to pay more because of who you are? You could be, as you were probably subjected to Online Price Personalization (OPP).

Is this practice lawful, since it (at least) seems to make consumers uncomfortable?[1]

As this article will try to demonstrate, the example above amounts to one of the simplest and less intrusive currently used forms of OPP, based on a consumer's purchase history in said trader's website. In fact, it is safe to assume (and, arguably, not too shocking for consumers) that traders retain information about their customers' past purchases, notably for accounting and tax purposes. What may feel unacceptable for consumers is to be served with a higher price for the same goods than their next-door neighbor, just because the trader uses said information to calculate his/her willingness to pay (WTP) a premium over the normal price.[2] On the other hand, the idea that consumers are more suspicious of data-intensive forms of OPP and that they are more willing to accept OPP if it works to their advantage (ie leading to price reductions) is under debate and needs further study.[3]

What if the information used by a certain trader to adjust the price which is shown to you would not be limited to what you had purchased from that trader before? What if the price "tag" would be calculated by checking these purchases against the location of the device you have been using to access the website over the last 6 months and the websites you visited that week? What if the trader, from that information, infers – accurately or not – that you live in a distant EU country, are experiencing financial trouble, belong to an ethnic minority

[1] In a 2005 survey conducted by Turow, "87% of respondents thought that it was wrong to charge different people different prices online for the same product during the same hour [and] 84% thought that websites ought to inform customers if they engaged in discriminatory pricing", as noted by A A Miller in 'What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing' (2014) Journal of Technology Law and Policy Vol. 19, 87. See J Turow & L Feldman, 'Open to Exploitation: America's Shoppers Online and Offline' (2005), Annenberg School of Communications, 6–12. In another study conducted by Turow and others, 78% of the respondents did not want "discounts (…) tailored for you based on following (…) what you did on other websites you have visited". See J Turow and others, 'Americans Reject Tailored Advertising and Three Activities that Enable it' (2009), available at http://ssrn.com/abstract=1478214, consulted on 28th May 2020.

[2] As noted by EU officials, "if a consumer finds out after having made a purchase that the price paid was higher than what other consumers paid, personalised pricing may have a negative impact on the reputation of the seller which may result in lost revenue". See OECD (Directorate for Financial and Enterprise Affairs Competition Committee), *Personalised Pricing in the Digital Era – Note by the European Union* [2018], 6.

[3] Some scholars argue that not only when consumers are economically disadvantaged by OPP do they feel unease with such practices. To quote Priester, Robbert and Roth, "In the face of similar transactions, an experienced price difference leads to the feeling of inequality and negative fairness perceptions" from the consumer. "A judgment of unfairness is generally associated with negative feelings such as unease or guilt when the inequality is to the buyer's advantage". See A Priester, T Robbert & S Roth, 'A special price just for you: effects of personalized dynamic pricing on consumer fairness perceptions' (2020) Journal of Revenue and Pricing Management 19, 99–112, 104 and 105. Zuiderveen Borgesius & Poort also argue that "The mere fear or suspicion of paying a premium could cause people to dislike personalized pricing". See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) Journal of Consumer Policy 40, 347–366, 355.

or that you are gay and, for one or more of those reasons, decides to increase the prices you see? Would it make it better if the trader used those types of information to decrease your price, instead?

Despite ethical concerns raised by OPP and the public and media scrutiny[4] every time OPP practices are revealed, there are not many rules directly addressing OPP in EU law. In fact, legal scholars tend to claim that under the existing framework, OPP per se is not unlawful, unless – and only to the extent that – it incidentally breaches rules relating to competition, anti-discrimination, data protection or consumer law.[5]

Although reports of OPP have surfaced since the beginning of the 21st-century[6], and that OPP's effects on consumer welfare have been called into question[7], only in late 2019 did the EU legislator specifically address the issue, with a view to reducing the information asymmetry[8] between traders deploying OPP techniques and the targeted consumers. But is merely forcing traders to inform consumers about the use of OPP enough to protect them from unfair practices in this regard?

This paper will try to outline how the newly enacted Omnibus Directive, as well as other existing EU law instruments, may be leveraged to shield consumers[9] against these controversial practices. It is divided into 5 parts: the first (I) is devoted to defining OPP – distinguishing it from other close phenomena – and pricing algorithms; the second (II) will look into the transparency requirement stemming from the Omnibus Directive and the worries that remain; the third (III) will briefly point out whether and how EU anti-discrimination laws are up to the task; the fourth (IV) shall argue that EU privacy and data protection law may pose serious hurdles to merchants who deem to use pricing algorithms; and the fifth (V) will explore how OPP may constitute, in some cases, unfair commercial practices, forbidden under the UCPD.

Due to time limitations, the paper will not dive into the implications of EU competition law to OPP. Some authors, however, argue that constrains to OPP from this field of law are unlikely to arise if the trader deploying it does not have a dominant position in its market and abuses said position – under Article 102 of the Treaty on the Functioning of the

---

[4] See, as examples, Harvard Business Review, *How Retailers Use Personalized Prices to Test What You're Willing to Pay*, 20th October 2017, available at https://hbr.org/2017/10/how-retailers-use-personalized-prices-to-test-what-youre-willing-to-pay, consulted on 26th May 2020; and Time, *Orbitz Shows Higher Prices to Mac Users*, 26th June 2012, available at https://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/, consulted on 26th May 2020.

[5] For further notes on the lawfulness of OPP, see F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3); L Drechsler & J C Benito Sánchez, 'The Price Is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms' (2018) European Journal of Law and Technology 9(3); J A Gerlick & S M Liozu, 'Ethical and legal considerations of artificial intelligence and algorithmic decision-making in personalized pricing' (2020) Journal of Revenue and Pricing Management 19, 85–98; and A M Sears, 'The Limits of Online Price Discrimination in Europe' (2020) The Columbia Science & Technology Law Review Vol. XXI.

[6] The first notable OPP "scandal" was the Amazon 2000 initiative to offer online shoppers prices tailored to their unique characteristics, which ended up with the company refunding its outraged customers. See P Krugman, Reckonings; What Price Fairness?, The New York Times, 4th October 2000, available at https://www.nytimes.com/2000/10/04/opinion/reckonings-what-price-fairness.html, consulted on 1st June 2020.

[7] See OECD, *Personalised Pricing* (n 2), 5.

[8] According to Zuiderveen Borgesius & Poort, "Transparency about which companies engage in price personalization could mitigate this information asymmetry: Consumers may choose online shops that do not personalize prices". See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 359.

[9] We will focus on consumer OPP only, and not OPP affecting customers making purchases or shopping around online for purposes included in their trade, business, craft or profession. See Article 2(1) of the CRD.

European Union –, which may be challenging to prove in a given case of OPP.[10]

I will neither address OPP from economical, sociological nor psychological points of view, although these may be occasionally brought to the discussion to beef up certain legal arguments.

1. Defining Online Price Personalization (OPP).

For the purposes of this paper, OPP shall be defined as the possibility of offering different prices to specific consumers for the same product, equal to each consumer's presumed maximum willingness to pay (WTP) for that product, which are automatically calculated and presented to consumers by a pricing algorithm.

In turn, a price algorithm shall mean a well-defined computational procedure that takes some value, or set of values, as input to determine price as an output for a particular consumer. These "values" are, normally, consumers' unique characteristics (eg. "iPhone user", "IP address from Orahovica, Croatia", "visited diageo.com twice in the last 24 hours") – or labels/profiles based on such characteristics (eg. "Wealthy Mother", "Remote location", "Occasional Drinker") which inform the decision taken by the pricing algorithm. More complex pricing algorithms may consider additional factors other than the consumer's WTP, such as the cost of delivering goods or services to the consumer's location or the likelihood that a specific consumer (eg. given his/her putative age, credulity or need) will become a long-time customer.

Although some authors argue that pricing algorithms are widely used across the internet[11], evidence shows otherwise.[12] Miller, more cautiously, claims that "because of the prevailing secrecy in the consumer data industry, it is a matter of conjecture how businesses actually translate the detailed profiles (…) into individual price offers, and how widespread these practices are."[13]

The author also delves into the data brokerage industry, making it clear that many online traders deploying pricing algorithms rely on third party-built customer profiles to target consumers with personalized prices. These data brokers use a variety of tracking technologies (such as cookies, web beacons, pixels and device fingerprinting) to follow internet users' digital trail. By combining this wealth of data "with advanced data-mining techniques [it is possible to] discover associations and connections between demographic characteristics and preferences for products, or (…) [to] predict consumers' reactions to changes in price or special deals"[14].

Often, traders will count on those or other (such as data analytics) companies'

---

[10] See Sears, 'The Limits of' (n 5), 8-14, and I Graef, 'Algorithms and fairness: What role for competition law in targeting price discrimination towards end consumers?' (2018) Columbia Journal of European Law 24 (3), 542-554.

[11] Drechsler & Benito Sánchez argue that "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". See Laura Drechsler & Benito Sánchez, 'The Price is (Not) Right' (n 5), 1.

[12] See OECD, *Personalised Pricing* (n 2), 7: "personalised pricing does not seem to be present in the EU on any significant scale, at least for the moment". See also Ipsos, London Economics & Deloitte, *Report for DG JUST "Consumer market study on online market segmentation through personalised pricing/offers in the European Union"* [2018], available at https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf, consulted on 1st June 2020, 260 and 261.

[13] Miller, 'What Do We Worry' (n 1), 51 and 52.

[14] ibid 49. See also Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 262: "e-commerce websites that want to personalise results do not always collect and subsequently process consumer data/profiles themselves; instead they often use specialised companies' personalisation or analytics software or services."

personalization software "for the optimization of their (…) pricing strategy" and to ensure each consumer is served with a personally tailored price when they visit their websites.[15] The incorporation of AI (namely, machine learning) in these pricing algorithms "for detecting patterns in data collected on consumers' purchasing history, product and pricing preferences (…) can be used for predictive recommendations, offers and prices."[16] Even if they may issue generic instructions to said companies about the way they deem to target their customers for OPP purposes, traders are frequently not aware of the details of the functioning of the pricing algorithms, notably of the types of data which are fed into them and of the logic involved in the automated pricing decision-making, as those are the suppliers' "closely guarded trade secrets."[17] As we shall see below, this may pose challenges to traders vis-à-vis their transparency legal obligations towards consumers relating to OPP.

Although many authors[18] use the term online price discrimination when referring to what we described above as OPP, it is important, to ensure that an unbiased view of the phenomenon of OPP is kept, to distinguish between both practices. Even if price discrimination practices also rely on the collection and analysis of data about potential or current customers to define a price for those specific customers, those differentiate between customers or groups of customers – for price tailoring purposes – based on very sensitive observed or inferred characteristics of those customers, specially protected under EU anti-discrimination law. These characteristics include customers' gender, race, nationality and place of residence[19]. The European Commission (EC) Guidance on the application of the UCPD also makes a similar distinction between both concepts, clarifying that "Price discrimination is where a trader applies different prices to different groups of consumers for the same goods or services"[20]. The Guidance then mentions some grounds based on which direct or indirect[21] discrimination is forbidden, such as the ones highlighted above.

---

[15] Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 262. On page 78, the report mentions several companies offering this type of services (such as HayStacks and Tajitsu).

[16] ibid 97.

[17] Miller, 'What Do We Worry' (n 1), 51. Wachter & Mittelstadt argue that that the definition of "trade secret" in Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive) is broad enough to include algorithms, customer profiles derived from said algorithms and forecasts about a customer's future life (i.e., derived and inferred data). See S Wachter & B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review Vol. 2019 Issue 2, 117-119.

[18] See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), and Sears, 'The Limits of' (n 5). Sears also states (6) that "Others prefer the term "price differentiation" in order to avoid the negative connotation of "discrimination." This may be commendable, as there are economic arguments that price discrimination may increase the total welfare of consumers and sellers."

[19] See Chapter III below for an analysis of these forbidden grounds of discrimination under EU law. Also in line with this distinction, see the letter by the Ministerie van Justitie en Veiligheid, *Moties op het terrein van gegevensbeschermingof* [2020], available at https://t.co/6aISm1DUp2?amp=1, consulted on 3rd June 2020, 2.

[20] EC, *Staff Working Document SWD(2016) 163 final Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices* [2016], 133.

[21] According to Article 2(2) of the Race Equality Directive (RED), "direct discrimination" shall be taken to occur where one person is treated less favorably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin, while "indirect discrimination" shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons. Thus, when a pricing algorithm takes a consumer's ethnic origin into account when making a pricing decision, this would be considered direct discrimination under the RED, including when it infers a certain consumer has a certain ethnic origin based on other observable aspects (eg. where the consumer lives, on the basis of his location history between 23:00h and 07:00h of each day over the course of a given month – see Judgement of 16th July 2015, *CHEZ Razpredelenie Bulgaria*, C-83/14, EU:C:2015:480, paragraph 59, ruling on inferences about Roma origin because of place of living). In turn,

Also relevant for the purposes of this paper is the distinction between first-degree price discrimination and third-degree price discrimination. According to Miller, "A first-degree price discrimination strategy requires that the firm be able to uniquely identify each consumer. It also requires a lot of information about the consumer's tastes and highest willingness to pay in order to tailor a price to an individual consumer[22]. (…) Third-degree price discrimination strategies require that the seller be able to identify at least whether the consumer has the relevant group trait that is used for discrimination, but does not necessarily need to uniquely identify consumers"[23].

Considering the above definition of OPP, first-degree price discrimination practices deploying pricing algorithms should also be considered as OPP practices. However, the same cannot be said of third-degree price discrimination, as the trader is not, in those cases, capable of singling-out a specific consumer through a unique identifier (eg. a cookie ID). The EU has recently taken the view that "The effect of first-degree price discrimination on consumer welfare is more likely to be harmful than third-degree price discrimination, because the producer captures up [or intends to capture up] to the entire surplus for all consumers, leaving them with potentially no gains from trade."[24]

It is also appropriate to separate OPP from dynamic pricing practices. Following the EC's Guidance on the UCPD, the latter means "changing the [displayed] price for a product in a highly flexible and quick manner in response to market demands". An example of this practice could be offering different prices in the same website, for the same products, at different times of the same days or different days of the same week, by raising the price when demand is surging or when supply in scarce[25]. Even if it has been reported[26] that consumers sometimes confuse OPP with dynamic pricing, the latter practice does not seem to draw significant concerns from the EU legislator, as the new information requirement stemming from the Omnibus Directive (which is analyzed in Chapter II below) does not apply to

---

algorithmic decision-making having a disproportionate impact on consumers of a certain ethnic origin without an objective justification would be considered indirect discrimination. See also the concept of "discrimination by association" in some EU Member-States laws (such as Portugal's Law no. 93/2017, of 23rd August, in Article 3(1)(d)), generally defined as discrimination which occurs because of one's relationship or association with a person or group of persons with certain specially protected characteristics (such as race, ethnicity or nationality). For more on how discrimination by association is often forbidden under EU law and the related CJEU's case law, see Wachter S, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) Berkeley Technology Law Journal Vol. 35 No. 2 (Forthcoming), 31-46.

[22] Zuiderveen Borgesius & Poort argue that "First-degree price discrimination refers to a situation in which each consumer is charged an individual price equal to his or her maximum willingness to pay. For first-degree price discrimination, the seller needs precise information about the buyer's willingness to pay (the reservation price). (…) In practice, such an extreme form of price discrimination will never occur, as sellers cannot learn the buyer's exact reservation price". F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 351. On a similar note, see OECD, *Personalised Pricing* (n 2), 3: ""Perfect" price discrimination would mean charging each person the price that reflects their exact personal maximum willingness to pay. This is also known as "first-degree" price discrimination. Perfect first-degree price discrimination is unlikely to occur in practice." There are strong arguments, however, to support the view that, for first-degree price discrimination to occur, a trader does not need to know with absolute certainty the targeted consumer's WTP, but merely to attempt to calculate this individual WTP, based on the information at its disposal about the targeted consumer.

[23] Miller, 'What Do We Worry' (n 1), 56 and 57.

[24] See OECD, *Personalised Pricing* (n 2), 5.

[25] See EC, *Staff Working Document* (n 20), 132. See also Priester, Robbert and Roth, 'A Special Price' (n 3), 99: [dynamic pricing] "entails price changes over time due to fluctuations in supply, demand, competition, or other factors. Prices thus vary depending on the time of purchase but are the same across consumers at a given time".

[26] See The Guardian, *How much…? The rise of dynamic and personalised pricing*, 20th November 2017, available at https://www.theguardian.com/global/2017/nov/20/dynamic-personalised-pricing, consulted on 26th May 2020.

dynamic pricing.[27]

Lastly, OPP should not be mistaken for personalized ranking, which may be defined as the technique of altering of the order in which available options are displayed to users in e-commerce websites to suit their perceived interests and preferences.[28] This practice also entails the processing of data about each visitor and may even "entail an element of personalised pricing if the options ranked highest are actually there to fit the person's maximum willingness to pay"[29]. As increasing evidence about the ubiquity of personalized ranking has been recently found[30], this has also been addressed by the EU legislator in Article 4(5) of the Omnibus Directive, which establishes an obligation for merchants to inform consumers about the main parameters determining [this] ranking.

Now that a definition of OPP has been provided, the ensuing Chapter will plunge into how the Omnibus Directive tackles OPP, how traders should go by informing consumers about the use of pricing algorithms and whether this transparency duty suffices to empower consumers to take informed decisions.

2. The Omnibus Directive: an insufficient shield against OPP.

As part of the New Deal for Consumers[31], which was announced in April 2018, the Commission published a Directive Proposal[32] to, among other objectives, update certain aspects of the CRD in relation to traders' information duties towards consumers. This Proposal eventually led to the adoption of the Omnibus Directive, on 27th November 2019, whose information requirements on OPP will be analyzed below.

The original text of the Proposal did not contain any reference to OPP. However, the EP proposed (in first reading) certain amendments to the Proposal in early 2019, notably suggesting the incorporation of an additional information requirement in Article 6 of the CRD, which would require the trader to inform the consumer about "whether and how algorithms or automated decision making were used, to present offers or determine prices, including personalised pricing techniques."[33] The wording of this requirement was then

---

[27] See Recital (45) of the Omnibus Directive. This does not mean, however, that certain dynamic pricing practices may not be considered as unfair commercial practices in certain circumstances, as pointed out by the EC: "A dynamic pricing practice where a trader raises the price for a product after a consumer has put it in his digital shopping cart could be considered a misleading action under Article 6(1)(d) UCPD." See EC, *Staff Working Document* (n 20), 133.

[28] See OECD, *Personalised Pricing* (n 2), 3.

[29] ibid. This practice is also known as "price steering". For further insights on the matter, see A Hannak and others, 'Measuring price discrimination and steering on ecommerce web sites' (2014) Proceedings of the 2014 Conference on Internet Measurement Conference, 305–318

[30] See Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 42 and 43.

[31] See EC, *Review of EU consumer law - New Deal for Consumers* [2018], available at https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en, consulted on 23rd May 2020.

[32] EC, *Proposal for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules, COM(2018) 185 final* [2018].

[33] EP, *Report on the proposal for a directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules (COM(2018)0185 – C8-0143/2018 – 2018/0090(COD))* [2019]

tweaked by the Council, which also inserted Recital (45) into the text[34]. Both would make their way to the final version of the Omnibus Directive.

Article 4(4)(ii) of the Omnibus Directive obliges traders to inform consumers, "where applicable, that the price was personalised on the basis of automated decision-making". Recital (45) of the Directive adds that "Traders may personalise the price of their offers for specific consumers or specific categories of consumer based on automated decision-making and profiling of consumer behaviour allowing traders to assess the consumer's purchasing power. Consumers should therefore be clearly informed when the price presented to them is personalised on the basis of automated decision-making, so that they can take into account the potential risks in their purchasing decision."

This approach recognizes how difficult it is for consumers to spontaneously realize that OPP is actually happening[35], and is in line with the EU legislator's tendency to protect consumers via evermore extending information duties incumbent upon traders.[36] On this particular matter, even before the enactment of the Omnibus Directive, Zuiderveen Borgesius & Poort have argued that traders were already obliged to inform consumers about the processing of their personal data for OPP purposes under the applicable privacy and data protection laws[37], in a clear and specific fashion[38]. However, despite the fact that, for traders, this new information requirement may feel like an unnecessary repeated burden, the advantage – for consumers – of having a specific information duty regarding OPP in the CRD relates to the legally required salience of the information under Article 6(1) of the CRD. In this regard, although the way in which traders will, in practice, comply with this information duty (eg. on the placement of OPP warnings and the level of detail of the information provided) is still a matter of conjecture,[39], it is already possible to draw some predictions.

The EC has recently stressed that, for the purposes of Article 4(4)(ii) of the Omnibus Directive, "The information about personalisation should be provided every time a personalised price is offered"[40]. This may mean that an "OPP tag" should be provided next to the displayed price. There is a chance that the industry will develop certificates or labels

---

[34] The amendments proposed by the Council, on 29th March 2019, may be found at https://www.europarl.europa.eu/RegData/commissions/imco/lcag/2019/03-29/IMCO_LA(2019)003440_EN.pdf, consulted on 23rd May 2020.

[35] In many cases, consumers may assume that, by seeing different prices on the same websites in two different visits when using the same device, they are being subject to OPP, when traders may be only experimenting with dynamic pricing (according to the time of the day, eg.). Users are more likely to detect OPP when they visit the same web shop using two different devices at the same time. But, then again, not all consumers have two different devices with internet access at their disposal to test this and the average consumer is not expected to be so diligent.

[36] See also See also Recital (2) of Services Directive: "A free market which compels the Member States to eliminate restrictions on cross-border provision of services while at the same time increasing transparency and information for consumers would give consumers wider choice and better services at lower prices." Evidence suggests, however, that this approach has been failing EU consumers. In a 2011 EC Special Barometer, more than a third of consumer respondents declared he or she was poorly informed about their rights as consumers and only 2% of respondents answered correctly to a set of questions relating to cooling-off periods, guarantee validity rights and unfair commercial practices. See EC, *Special Eurobarometer 342 / Wave 73.2 & 73.3. – TNS Opinion & Social* [2011].

[37] Notably, under Article 5(3) of the ePrivacy Directive and Articles 13(2)(c) and 14(2)(c) of the GDPR.

[38] See F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 359.

[39] As Member-States are only required to transpose the Omnibus Directive by 28th November 2021 and to start applying the new rules from 28th May 2022. See Article 7(1) of the Omnibus Directive.

[40] EC, Recommendations for a better presentation of information to consumers (updated) [2019], available at https://ec.europa.eu/info/sites/info/files/sr_information_presentation.pdf, consulted on 26th May 2020, 10, n 18.

to indicate to consumers that the price they are seeing online has been calculated by a pricing algorithm. Alternatively, the Commission may also publish a template for the display of this information, as it already did with the current set of requirements of Article 6(1) of the Consumer Rights Directive[41].

What seems clear is that, in line with the general requirements of the CRD, information about OPP should be displayed "in a way appropriate to the means of distance communication used in plain and intelligible language"[42]. Furthermore, as generally the trader deploying OPP shall enter into a distance contract with the consumer for the selling of goods or the provision of services, the former is required to "make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1)."[43] As information relating to OPP relates to price (which, in turn, is mentioned in indent (e) of Article 6(1) CRD) and given the Omnibus Directive has inserted this new information requirement as indent (ea) to Article 6(1), it is safe to assume that also the foregoing type of information should be provided in such a clear and prominent manner, and right before the consumer clicks the 'buy' button[44].

Given that consumers have a limited attention span for information provided by a trader before placing their orders, as they tend to avoid information overload by focusing on the elements which they consider to be more important (including price)[45], legally mandating traders to provide information about OPP in a salient manner such as this could help consumers take more conscious decisions about whether or not to engage with merchants deploying pricing algorithms. The effects of OPP tags on consumer purchasing habits are yet to be seen, however, as there is a chance they will largely be ignored by motivated buyers. Still, due to this new information requirements, and since consumers are known to be skeptical about OPP (see note 1), law-abiding online traders may be discouraged to deploy or keep using pricing algorithms, fearing consumers would disengage upon acknowledging they may be targeted with different prices than other consumers based on their personal characteristics.

Furthermore, the dissemination of OPP tags in online marketplaces and shops would create an opportunity for third-party auditors, policymakers, consumer associations and regulators alike to assess how widespread OPP practices are, which could prove useful for designing advocacy, regulatory or enforcement strategies for or against them.

Despite the adoption of the Omnibus Directive, however, concerns about OPP remain. Notably, and as outlined above, the level of detail of the information that traders are required to provide via OPP tags is not thoroughly defined in the Omnibus Directive. In this respect, there are arguments for keeping these tags very simple, much like warning labels, without

---

41 See Annex I of EC, *DG Justice Guidance Document concerning 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* [2014].

42 Article 8(1) CRD.

43 Article 8(2) CRD. According to Recital (39) CRD, these information elements should "be displayed in the close vicinity of the confirmation requested for placing the order". The EC adds that "the terms 'prominent manner' and 'close vicinity' in Recital (39) suggest stronger requirements on presenting information compared to the general requirements under Article 6(1) and 8(1). The information should be presented in a way that the consumer can actually see and read it before placing the order without being obliged to navigate away from the page used to place the order." See EC, *Recommendations* (n 40), 32.

44 The EC has clarified that "Article 8(2) of the Directive would in practice apply at the moment in which the consumer is asked to verify the order in line with the eCommerce Directive, i.e. to check the contents of the shopping basket before clicking on the 'buy' button". See EC, *Recommendations* (n 40), 32.

45 See M Vieira Ramos, 'Psicologia e Direito do Consumo: a Proteção do Consumidor face aos Efeitos das Modernas Práticas Comerciais' (2019) Anuário do Nova Consumer Lab 2019, 335-492, 345 and 346.

any details regarding the functioning of the pricing algorithm, so as to not overwhelm consumers with information and ensure the tags' effectiveness. This, however, may be in contradiction with the traders' transparency duties under the GDPR regarding automated decision-making (as detailed in Chapter IV, below).

Moreover, in a December 2019 question to the EC – which may well reflect the public suspicion of OPP –, a Member of the EP observed that "AI can be used to engage in far-reaching individual online price discrimination (personalization of prices) based on consumer data such as location, purchasing history, surfing behavior, etc.", and queried whether the EC was aware of this type of practices and if it was "considering a general prohibition on online price discrimination"[46]. In his March 2020 answer, EC's Justice Commissioner Didier Reynders highlighted that practices such as online price discrimination, dynamic pricing and OPP are regulated under several EU law instruments, from the EU's anti-discrimination, privacy, data protection and consumer acquis. Therefore, even if such practices are not forbidden per se, the EC committed to monitoring "the prevalence of online price discrimination and, if necessary, [to] take further action to ensure a high level of consumer protection."[47],

Having that said, the article now elaborates on how the EU's anti-discrimination laws protect consumers against unjustified online price discrimination and, therefore, certain forms of OPP.

3. The EU anti-discrimination framework: limited safeguards and a heavy burden of proof.

The EU's primary law directly refers to non-discrimination on several provisions. Article 2 of the Treaty on the European Union states that "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail." Article 3 adds that the EU shall "combat social exclusion and discrimination", as well as promote "equality between women and men". Articles 10, 18, 19 of the Treaty on the Functioning of the European Union (TFEU) also refer to the EU's goal to combat discrimination, notably based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. Article 21 of the Charter of Fundamental Rights of the European Union (CFREU)[48] further prohibits discrimination "based on any ground such as sex, race, color, 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", as well as nationality.

In principle, EU primary law instruments such as the ones cited are only binding for EU institutions and their Member-States, and not for private parties.[49] The CJEU has, however,

---

[46] EP, Question for written answer E-004289/2019 to the Commission, by Kris Peeters (MEP), 9th December 2019, available at https://www.europarl.europa.eu/doceo/document/E-9-2019-004289_EN.html, consulted on 23rd May 2020.

[47] EC, *E-004289/2019 Answer given by Mr Reynders on behalf of the European Commission* [2020], available at https://www.europarl.europa.eu/doceo/document/E-9-2019-004289-ASW_EN.html, consulted on 23rd May 2020.

[48] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.

[49] Article 51(1) of the CFREU states that "The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law." The CJEU has ruled that, for EU primary law to have horizontal direct effect (i.e., to bind private entities), it must create precise, clear and unconditional obligations for private entities,

pointed out the horizontal effect of certain primary EU law provisions, namely when a general principle of EU law – such as the principle of non-discrimination on grounds of age[50] or on grounds of religion or belief[51] – is at stake.

Despite the above considerations, traders deploying OPP will mostly look into other more densified EU legislative instruments – such as Regulations[52] and Decisions[53] - to understand what their obligations regarding OPP are. This is without prejudice to EU Member-State law transposing the EU's Directives[54], which is directly applicable to such players.[55]

The EU has passed some legislative instruments which, if duly enforced at Member-State level, may be liable to prevent traders from carrying out online price discrimination. The Race Equality Directive (RED), which applies to "all persons, as regards both the public and private sectors", prohibits the discrimination of individuals, when accessing goods or services, on grounds of their racial or ethnic origin[56]. However, even if, at first sight, this Directive seems like a viable tool for consumers who have been online targeted with a personalized price by reason of their observed or inferred ethnic or racial origin to seek compensation or other suitable remedies, Sears notes that "demonstrating that a person was discriminated against on the basis of race or ethnicity through online price discrimination may be quite difficult, in particular where algorithmic personalized pricing operates within a "black box"." Furthermore, if one considers that the plaintiff must also show "that the only reasonable explanation for the difference in treatment is [his/her] protected characteristic"[57] (under Article 8(1) of the Directive), then the RED ceases to look like such a bright avenue for consumers.

The same arguments are valid when we look at the protection awarded to consumers by the Gender Goods and Services Directive (GGSD)[58], with an additional nuisance related to

---

which do not call for additional measures. See Judgement of 5th February 1963, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*, 26-62, ECLI:EU:C:1963:1.

50 See Judgement of 19th January 2010, *Seda Küçükdeveci v Swedex GmbH & Co. KG*, C-555/07, ECLI:EU:C:2010:21, paragraphs 21 to 23.

51 See Judgement of 17th April 2018, *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV*, C-414/16, ECLI:EU:C:2018:257, paragraph 76.

52 See Article 288(2) TFEU.

53 See Article 288(4) TFEU.

54 See Article 288(3) TFEU.

55 The CJEU has consistently denied conferring horizontal direct effect to Directives, even when their respective deadline for Member-State transposal had already elapsed (see, *inter alia*, Judgement of 26th February 1986, *Marshall v Southampton and South-west Hampshire Area Health Authority*, 152/84, ECLI:EU:C:1986:84, paragraph 48). However, in what is known as the principle of indirect effect (or *principe d'interprétation conforme*), national courts are bound to interpret their domestic laws in accordance with any Directives whose transposition period has elapsed, as far as possible. See Judgement of 10th April 1984, *Von Colson v Land Nordrhein Westphalen*, 14/83, ECLI:EU:C:1984:153, paragraph 28, and Judgement of 13th November 1990, *Marleasing SA v La Comercial Internacional de Alimentacion SA*, C-106/89, ECLI:EU:C:1990:395, paragraph 8. In some cases, the CJEU has awarded indirect effect to Directives whose transposition period had not yet elapsed, when general principles of EU (such as non-discrimination) were at stake. See note 146, below.

56 Article 3(1)(h) of the Race Equality Directive. According to CJEU case law, this shall include the provision of healthcare services. See Judgement of 12th July, *B.S.M. Geraets-Smits v Stichting Ziekenfonds VGZ and H.T.M. Peerbooms v Stichting CZ Groep Zorgverzekeringen*, C-157/99, ECLI:EU:C:2001:404, paragraph 55.

57 See Sears, 'The Limits of' (n 5), 31 and 33.

58 The GGSD lays down a framework for combating discrimination based on sex in access to and supply of goods and services and applies to all persons who provide goods and services (Articles 1 and 3(1) GGSD). The CJEU has ruled that considering the gender of the insured individual as a risk factor in insurance contracts constitutes discrimination, thereby invalidating former Article 5(2) GGSD – which allowed for such discrimination. See Judgement of 1st March 2011, *Association Belge des Consommateurs Test-Achats ASBL and Others v. Conseil des ministres [GC]*, C-236/09, ECLI:EU:C:2011:100, paragraphs 30 to 33. See also Article 9(1) GGSD on the burden of proof.

the fact that national legislators and courts have transposed and interpreted the Directive with substantial differences[59] and, thus, not all EU jurisdictions grant the same level of protection to consumers against pricing algorithms which take a consumer's gender as a decisive factor.

As mentioned by Commissioner Reynders in his March 2020 letter (see note 47), Article 20(2) of the Services Directive also generally prohibits consumer discrimination on the basis of their nationality or place of residence when accessing services[60]. Aimed at bolstering cross-border trade[61], but arguably still applicable in intra-EU Member-State transactions between traders and consumers, this prohibition is without prejudice to the traders' possibility of invoking objective criteria for offering different prices to different consumers for the same products or services on the basis of each consumer's location (which may be obtained from the consumer's device GPS coordinates – if their use has been consented by the consumer[62] – or from the device's IP address). These criteria may be linked to "additional costs incurred because of the distance involved[63] or the technical characteristics of the provision of the service, or different market conditions, such as higher or lower demand influenced by seasonality, different vacation periods in the Member States and pricing by different competitors, or extra risks linked to rules differing from those of the Member State of establishment", or the lack of the required intellectual property rights in the territory where the goods should be delivered.[64]

It is noteworthy that, out of the 532 complaints received by the European Consumer Centres Network (ECC-Net) between January 2013 and December 2015 related to Article 20(2) Services Directive discrimination, 68% of them were connected with "price or service differentiation [in] the purchase of goods, such as electronic goods, household appliances, vehicles, clothes, books, music or data downloads."[65] ECC-Net's report further noted that consumers often struggle to identify and find the contact details of the adequate enforcement bodies.[66] Gathering relevant documentary evidence to support consumers' claims may be

---

[59] On this, see Sears, 'The Limits of' (n 5), 32.

[60] The CJEU has made clear that this prohibition extends to the activity of retail trade in goods. See Judgement of 30th January 2018, *College van Burgemeester en Wethouders van de Gemeente Amersfoort v. X BV (C-360/15), and Visser Vastgoed Beleggingen BV v. Raad van de Gemeente Appingedam (C-31/16)*, Joined Cases C-360/15 and C-31/16, ECLI:EU:C:2018:44, paragraph 97. In turn, the EC points to the concept of "service" under Article 57 TFEU and offers a non-exhaustive list of services covered by the Directive, including "distribution of goods and services (retail), services in the field of tourism such as travel agencies, leisure services (…), the organisation of events, advertising and recruitment services." See EC, *Staff Working Document SWD(2012) 146 final with a view to establishing guidance on the application of Article 20(2) of Directive 2006/123/EC on services in the internal market ('the Services Directive') Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the implementation of the Services Directive: A partnership for new growth in services 2012-2015* [2012], 9.

[61] See M Karlson Jernbäcker, 'Article 20 (2) of the Services Directive - A prohibition against consumer discrimination' (2014) Uppsala University.

[62] See Article 9(1) of the ePrivacy Directive.

[63] However, the EC has stated that failure to supply due to lack of delivery options, due to the contractual relationship between independent undertakings, or due to higher charges for cross-border payments (in euro) are unlikely to be accepted as objective reasons for offering higher prices to consumers. See EC, *DG Internal Market and Services IMCO Working Group on the Digital Single Market, Article 20(2) Services Directive* [2013], available at https://www.europarl.europa.eu/document/activities/cont/201303/20130314ATT63206/20130314ATT63206EN.pdf, consulted on 1st June 2020.

[64] See Recital (95) of the Services Directive.

[65] ECC-Net, *Do Invisible Borders Still Restrict Consumer Access to Services in the EU?* [2017], available at https://ec.europa.eu/internal_market/scoreboard/_docs/2017/european_consumer_centre_network/services-directive-report_en.pdf, consulted on 1st June 2020, 6.

[66] ibid 45.

particularly difficult in Article 20(2) Services Directive-related online price discrimination, as consumers would need to demonstrate (i) they are being subject to online (first or third-degree) price discrimination and (ii) that said discrimination is occurring solely on the basis of their location.[67] This may become easier once the Omnibus Directive transparency requirement on OPP is transposed into Member-States' laws, especially if this leads to traders providing meaningful information to consumers about the variables considered by the pricing algorithm in cases where location is the sole one (which is unlikely to be the case).

More recently, the Geo-Blocking Regulation was approved to prevent "unjustified geo-blocking and other forms of discrimination based, directly or indirectly, on the customers' nationality, place of residence or place of establishment, including by further clarifying certain situations where different treatment cannot be justified under Article 20(2) of [the Services Directive]."[68] Unlike the Services Directive, it clearly states that it does not apply to purely internal situations, where all the relevant elements of the transaction are confined within one single Member State.[69] While Gerlick and Loizu argue that the Geo-Blocking Regulation "eliminates one conduit through which such practices are facilitated, notably, discrimination on grounds of the consumer's place of residence"[70] (restricted to the access of goods or services mentioned in Article 4(1) of the Regulation), Sears holds that the Regulation "does not mandate the complete harmonization of prices. Different prices, offers, and conditions may be given to customers in certain scenarios, so long as it is nondiscriminatory. For example, a business could sell a product for a different price in its physical stores as compared to its website."[71] In a recent EC-conducted screening of nearly 500 e-shops selling clothing and footwear, furniture and household items, and electric appliances, "One fifth of the flagged websites did not respect the Geo-blocking Regulation which allows consumers to shop from websites not delivering in their country of residence, provided they can get it delivered to an address in the country served by the trader i.e. the "shop like a local principle"."[72]

There are also other sectoral EU legal instruments (notably, in the air[73], maritime[74] and coach[75] transport sectors) which may grant specific protection to consumers against nationality or location-based OPP when accessing certain types of services.

All in all, and going back to the text of Article 21 CFREU, it is safe to say that the EU legislator has (to date), in what concerns its anti-discrimination acquis, fallen short of ensuring comprehensive protection to EU consumers against OPP based on assumedly commonly-used factors/unique characteristics, such as language, religion or belief, political or any other opinions, property (i.e., wealth or lack thereof), disability (or health condition), age or sexual orientation. One may also point out that the burden of proof incumbent upon customers/plaintiffs for demonstrating they have been subject to online price discrimination

---

[67] Sears, 'The Limits of' (n 5), 32.
[68] Article 1(1) Geo-Blocking Regulation.
[69] Article 1(2) Geo-Blocking Regulation.
[70] Gerlick and Liozu, 'Ethical and Legal' (n 5), 90.
[71] Sears, 'The Limits of' (n 5), 35.
[72] EC, *Press Release "Online shopping: Commission and Consumer Protection authorities urge traders to bring information policy in line with EU law"* [2020], available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_156, consulted on 3rd June 2020.
[73] Article 23(2) of Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community.
[74] Article 4(2) of Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004.
[75] Article 4(2) of Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport.

under the currently existing laws seems to be an almost insurmountable obstacle for consumers wishing to enforce their rights in this space.

Regardless of the political factors which led to the aforesaid legislative inaction[76] and the legally prescribed burden of proof rules, it is expected that the EU will continue to push for the abolition of all types of discrimination in the supply of goods and services with a consumer-oriented view and in line with the Treaties[77]. In the meantime, it is of paramount importance to analyze what alternative tools EU law offers to consumers against OPP, starting with privacy and data protection laws.

4. EU Privacy and Data Protection law: a big hurdle for OPP.

OPP involves the collection, analysis and mining of information about consumers who visit online shops. This may include, depending on the characteristics of each trader's pricing strategy (and the model of the pricing algorithm), personal data[78] such as the consumer's name, other unique identifiers (such as cookie IDs or their device's IP or MAC Address[79]), purchase history via loyalty cards or in the trader's website, email address, phone number, location (eg. GPS data and Bluetooth sensor data), type of device and browser used to access the online shop, publicly available data (eg. land registry records), behavioral and interests data (eg. browser history, apps used, social media posts) and socio-demographic data (eg. age, gender, level of education, number and identification of household members).

The advent of tracking and data analytics technologies, bolstered by advances in computing power and, thus, decreases in the cost of collecting, storing and analyzing vast amounts of data, made it interesting for traders to try to maximize their profits by deploying pricing algorithms These algorithms are arguably capable of estimating each online consumer's WTP based on online profile(s) drawn from connections between multiple data points[80].

---

[76] Back in 2008, the European Commission proposed the so-called Horizontal Directive, which intended to ensure equal treatment between persons in the EU, irrespective of religion or belief, disability, age or sexual orientation, including with regards to the access to goods and services. Since then, twelve years have passed and the legislative process did not lead to the adoption of the Directive, arguably because it has been blocked by the Council. See Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation {SEC(2008) 2180} {SEC(2008) 2181}, of 2nd July 2008. See also Joint NGO Statement on the 10th Anniversary of the Horizontal Directive, *Ten years on and nothing to show for it* [2018], available at https://www.age-platform.eu/sites/default/files/HorizontalDirective_jointStatement_10th%20Anniversary-Jul2018.pdf, consulted on 5th June 2020.

[77] For a comprehensive view of the currently applicable anti-discrimination framework in Europe, see European Union Agency for Fundamental Rights (FRA), *Handbook on European non-discrimination law* [2018].

[78] Article 4(1) GDPR.

[79] Recital (30) of the GDPR states that "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

[80] See Authority for Consumers and Markets Authority, *Guidelines on the Protection of the online consumer - Boundaries of online persuasion* [2020], available at https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf, consulted on 3rd June 2020, 19: "Technological developments are enabling businesses to predict consumer behavior with increasing accuracy using personal and other data. For example, businesses are increasingly well informed about consumers' personal preferences and choices, in some cases better than the consumers themselves." See also Gerlick and Liozu, 'Ethical and Legal' (n 5), 86: "Businesses race to convert mountains of data into generative insights to improve personalization-centered retail practices. They deploy internally developed and acquired technology factors that enable the marketing function to bridge from customer segmentation to individual personalization."

Frequently, the data collection, analysis and mining, as well as consumer profiling[81] and price targeting via a pricing algorithm will not be conducted by the traders themselves, but by service providers on their behalf, like data brokers and data analytics companies (as outlined in Chapter I). However, this does not relieve traders from complying with their obligations as data controllers[82] vis-à-vis the consumer personal data processing for OPP, given that, in any case, they define the purpose of the processing of said data[83]. The fact that, in certain cases where the consumer tracking technologies and the pricing algorithm models are defined by external service providers, traders may not determine or have visibility on some essential elements[84] of the means of the data processing for OPP may be troublesome in that regard. According to the EDPB, where a service provider takes an active role in determining said essential means and the purpose of the data processing, it acquires a certain degree of (sole or joint) controllership[85], even if it enters into an agreement with a trader which formally qualifies it as a mere processor [86]. In those cases (notably, where service providers do not reveal to their customers – i.e. traders – all the sources and types of data their "proprietary" pricing algorithm shall use to reach a pricing decision), it is still not clear, under recent CJEU case law, whether traders shall be acting as independent or joint

[81] For the purposes of the GDPR, 'profiling' is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." See Article 4(4) of the GDPR. The analysis and prediction of said aspects tend to have a decisive impact on pricing decisions taken by pricing algorithms. See I Mendoza and L A Bygrave, 'The Right not to be Subject to Automated Decisions based on Profiling' (2017) University of Oslo Faculty of Law Research Paper No. 2017-20, 1: "[Profiling] methods are instituted for a variety of ends, such as enhancing the impact of advertising, screening applicants for jobs or bank loans, and creating differentiated pricing for services. Examples include online behavioural advertising, e-recruiting, and weblining." Also, according to Mendoza and Bygrave (2), 'weblining' includes, but is not limited to, OPP.

[82] Article 4(7) GDPR defines 'controller' as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[83] Those obligations include, among many others, ensuring that only the types of personal data which are strictly necessary are processed, that a legal basis (eg. consent) exists for carrying out the processing, that consumers (as data subjects) are informed about how their data is processed, that the processing of sensitive personal data or automated decision-making affecting data subjects is not forbidden in a given case, that data subjects are given the possibility of opting-out of profiling and that all third-parties involved in the data processing are bound by specific duties relating to data protection.

[84] The EDPB has stressed that these 'essential means' "are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller" and include, *inter alia*, the determination of the types of data which shall be processed, the categories of data subjects, for how long the data will be retained, as well as who shall have access to the data. See EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* [2020], 9.

[86] As stressed by the EDPB, "a merely formal criterion would not be sufficient", as "it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing". It is also possible to imagine, in the context of OPP, "a processor [that] infringes the GDPR by going beyond the controller's instructions [by] starting to determine its own purposes and means of processing" (eg. if the personalization services provider decides to collect additional types of data to build more detailed consumer profiles and to train its "proprietary" pricing algorithm), thereby acquiring a controller status regarding those specific processing operations. See WP29, *Guidelines 07/2020* (n 86), 17 and 25, and Article 28(10) GDPR.

controllers[87][88] with those service providers, in relation to the traders' website visitors' personal data. In the latter case, both parties would need to agree on which of them should inform consumers about the processing of their personal data for OPP purposes[89]. In cases where said service providers only define purely technical means[90] of the processing of the consumers' data for OPP purposes – thus firmly keeping their processor status –, traders may instruct those providers to assist them clarifying any questions consumers may have about the processing of their data by the pricing algorithm[91].

As controllers, for collecting and further processing (either directly or through third-party service providers) consumer data for OPP purposes, traders will need to make sure that a valid legal basis exists to that effect. While it is very unlikely that said processing may be considered necessary for entering into a contract with the consumer[92], and given that the WP29 has ruled out the possibility of relying on the legitimate interests' legal basis[93] for extensive profiling[94], "tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research"[95], it seems that traders have no choice but to rely on consumers' consent for OPP[96].

While the above is still open to some discussion (as controllers may admittedly still conduct some forms of non-intrusive profiling under the legitimate interests' legal basis), it is crystal clear that traders relying on tracking technologies which capture information from consumers' devices for OPP purposes (such as cookies, device fingerprinting or tracking pixels) must collect prior express[97] consent from the user, under Article 5(3) of the ePrivacy

---

[87] It seems more likely that such service providers would be qualified as joint controllers with the trader deploying OPP in its website, since, in principle, they shall be determining certain essential elements of the means of one or more data processing operations involved in OPP and will use the data to train their pricing algorithm, therefore pursuing their own business interests. This is irrespective of the fact that personalization service providers shall tailor prices on the basis of data observed (eg. via tracking pixels or geo-targeting) or inferred (eg. from browser searches) about consumers.. See Judgement of 29th July 2019, *Fashion ID GmbH & Co. KG, C-40/17*, ECLI:EU:C:2019:629, paragraphs 77 to 84, and EDPB, *Guidelines 08/2020 on the targeting of social media users* [2020], 20 and 23.

[88] It is safe to assume, however, that a given entity does not need to have access to the personal data to be considered as a controller jointly with the entity accessing the data, as long as both jointly determine the purpose and the means of the data processing. This shall often be the case of traders who employ personalization service providers for OPP purposes and never actually receive the raw data obtained and processed by said suppliers for that purpose. See Judgement of 10th July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 69.

[89] Article 26(1) GDPR.

[90] For instance, the way the data is stored in the providers' servers and protected against any risks, for the purposes of Article 32(1) GDPR, as well as the lines of code used to program the pricing algorithm strictly to fit the trader's pricing strategy.

[91] Article 28(3)(e) GDPR.

[92] See EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [2019], 9: "When assessing whether Article 6(1)(b) [GDPR] is an appropriate legal basis for processing in the context of an online contractual service, regard should be given to the particular aim, purpose, or objective of the service. For applicability of Article 6(1)(b), it is required that the processing is *objectively necessary* for a purpose that is integral to the delivery of that contractual service to the data subject."

[93] Article 6(1)(f) GDPR.

[94] See WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)*, of 9th April 2014, 18 and 26.

[95] WP29, *Opinion 03/2013 on purpose limitation (WP203)*, of 2nd April 2013, 46.

[96] With a similar view, see F Zuiderveen Borgesius & J Poort, 'Online Price Discrimination' (n 3), 361; Sears, 'The Limits of' (n 5), 21; Gerlick and Liozu, 'Ethical and Legal' (n 5), 90; OECD (Directorate for Financial and Enterprise Affairs Competition Committee), *Personalised Pricing in the Digital Era – Note by the BEUC* [2018], 9; and Ministerie van Justitie en Veiligheid, *Moties op het terrein* (n 19), 4.

[97] The CJEU has confirmed that the meaning of user "consent" in the ePrivacy Directive equates to the Article 4(11) GDPR concept of consent and, in line with Recital (32) GDPR, it ruled that pre-ticked checkboxes which are not un-ticked by a website user before continuing to browse the site do not constitute valid consent for the

Directive. A similar conclusion should be drawn where the trader processes the categories of personal data set-out in Article 9(1) GDPR – such as information revealing the consumer's racial or ethnic origin, religion, health condition or sexual orientation – for OPP purposes, even if those elements are merely inferred[98] from other data which are voluntarily provided by the consumer or observed by the trader[99] and regardless of whether said inferences are correct or not[100].

It is also highly discussed in academic literature whether OPP falls under the Article 22(1) GDPR definition of automated decision-making and, thus, whether OPP is forbidden, save for consumer explicit consent[101]. On the first issue, as rightly pointed out by Sears, "four conditions must be met for [Article 22] to apply. There must be (1) a decision (2) based solely (3) on automated processing of personal data that (4) results in legal or similarly significant effects on the individual."[102] If the fulfilment of the three first criteria by OPP is not contentious, authors have discussed whether OPP may have a legal or similarly significant effects on the data subject (in this case, the consumer being targeted with a personalized price). For Steppe, OPP does not have a legal effect on the consumer and shall only have a significantly similar effect in cases where the consumer is asked to pay a substantially higher amount[103]. More generously, Malgieri and Comandé take the view that the majority of pricing

placement of cookies or for using similar technologies. A similar argument should be drawn against the consideration of the mere display of an OPP tag, next to a personalized price, as any form of valid consent under the GDPR – it is not because a consumer has been shown an OPP tag that he or she accepts the processing of his or her personal by an intrusive pricing algorithm. See Judgement of 1st October 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, C-673/17, ECLI:EU:C:2019:801, paragraphs 55, 57 and 63. In the same line, see AG Spuznar Opinion of 4th March 2020, *Orange România SA*, C-61/19, ECLI:EU:C:2020:158, paragraph 60. Subsequent processing of the personal data which may be obtained via a cookie, however, may, in theory, be based on alternative legal bases under Article 6(1) of the GDPR. See, in this regard, EDPB, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* [2019], paragraph 41.

98 See Wachter & Mittelstadt, 'A Right to Reasonable Inferences' (n 17), 72: "when inferred or derived data directly disclose protected attributes—for example when a processor infers a person's ethnicity from their education history—they must be treated as sensitive data. (…) Second, when personal data can be shown to allow for sensitive attributes to be inferred (i.e., 'indirectly revealed'), the source data from which sensitive inferences can be drawn can also be treated as sensitive data (e.g. last name or location of birth to infer race)." See also WP29, *Advice paper on special categories of data ("sensitive data")*, Ref. Ares(2011)444105, of 20th April 2011, 6: "not only data which by its nature contains sensitive information is covered by [what today corresponds to Article 9(1) GDPR], but also data from which sensitive information with regard to an individual can be concluded."

99 On the distinction between inferred, observed and voluntarily provided data, see WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (*WP251rev.01)*, as last Revised and Adopted on 6th February 2018, 8; and Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 49.

100 In its Nowak ruling, the CJEU took a broad view on the definition of personal data, therein including data in the form of opinions and assessments, provided that they relate to the data subject. See Judgement of 20th December 2017, *Peter Nowak v. Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 34..

101 As Article 22(2)(a) and (b) GDPR are unlikely to be applicable in OPP involving automated decision-making.

102 See Sears, 'The Limits of' (n 5), 23.

103 R Steppe, 'Online price discrimination and personal data: A General Data Protection Regulation perspective' (2017) Computer Law & Security Review 33, 783. In agreement with Steppe, Bygrave claims that OPP shall only have such similarly significant effects with it represents "non-trivial economic consequences [for data subjects] (e.g. the data subject must pay a substantially higher price for services than other persons, effectively preventing her/him from accessing these services) – a fortiori if this occurs repeatedly". See L A Bygrave, *The EU General Data Protection Regulation (GDPR) – A Commentary* (1st edn, Oxford University Press 2020), 534. Both opinions seem to be in line with the position taken by the WP29 (and later embraced by the EDPB), as the latter holds that "For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential

algorithms represent automated decision-making having a similarly significant effect on data subjects[104]. The Belgian DPA inclusively held, back in 2011 (pre-GDPR), that OPP even produces legal effects for consumers when they are required to pay a premium (regardless of its amount).[105] On the second contentious matter, it now seems clear that Article 22(1) GDPR contains a general prohibition on decision-making based solely on automated processing, and not a subjective right for data subjects to object to said decision-making[106], in spite of the fact that the wording of Article 22(1) could suggest that the latter was the case.

So, if data subject consent[107] is required for OPP, how should traders be planning to obtain it? Will we witness a proliferation of "OPP banners" in traders' websites, which would pop-up once a visitor accesses the site, asking him or her to consent to OPP (just like cookie banners do[108] in relation to analytics and advertising cookies)? This would add a degree of complexity to the Omnibus Directive-mandated "OPP tags" (which were discussed in Chapter II), as they would be serving an additional purpose to merely informing consumers about OPP.

Traders could also consider adding a new purpose[109] (i.e., data processing for OPP) to their currently used cookie banners, although this would only cover the use of tracking technologies for OPP and not the collection of their data through other means (eg. scrapping of publicly available data by data brokers), the combination of all those data for consumer profiling and, ultimately, price tailoring. In both those cases, traders should avoid implementing OPP or cookie-walls (i.e., denying access to the site unless the user accepts OPP or non-essential cookies[110]), "nudging" techniques (eg. placing a big, bright colored "Accept" button and a small, grey "Reject" button in the banner) and assuming that a user

---

to: significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals." See WP29, *Guidelines on Automated individual decision-making* (n 102), 21.

[104] G Malgieri & G Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) IDPL 7, 243.

[105] Commission for the Protection of Privacy Belgium, *Opinion no. 35/2012 of the CPP's accord on the draft regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, of 21st November 2012, unofficial translation www.privacycommission.be/sites/privacycommission/files/documents/Opinion_35_2012.pdf, consulted on 3rd June 2020, paragraph 80.

[106] See WP29, *Guidelines on Automated individual decision-making* (n 102), 19 and 20.

[107] Consent should be "freely given, specific, informed (…) unambiguous" and given "by a statement or by a clear affirmative action". See Article 4(11) GDPR.

[108] Or should do. While some DPAs have recently taken the view that some first-party analytics cookies may be exempt from the ePrivacy Directive's consent requirement (such an the French DPA), both the Irish and the UK DPAs have stressed that analytics cookies are not strictly necessary for providing an information society service at the request of the user and, as such, may only be placed upon prior user consent. See Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019*, of 1st October 2020, available at https://www.cnil.fr/sites/default/files/atoms/files/ligne-directrice-cookies-et-autres-traceurs.pdf, consulted on 3rd October 2020; Data Protection Commission, *Guidance Note: Cookies and other Tracking Technologies* [2020], 7-8 ; and Information Commissioner's Office, *How do we comply with the cookie rules?*, available at https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply10, consulted on 4th June 2020.

[109] Matte, Santos and Bielova have denounced that websites relying on IAB Europe's Transparency and Consent Framework do not offer the user the possibility of consenting to the placement of cookies for purposes which are specific enough to meet the GDPR's purpose specification principle. See C Matte, C Santos, N Bielova, 'Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?' (2020) APF 2020 - Annual Privacy Forum, Oct 2020, Lisbon, Portugal, 1-24.

[110] See EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679* [2020], paragraphs 39 to 41.

who merely closed the banner without accepting or rejecting OPP or cookies has consented to their use[111]. In spite of all these requirements, it is possible that some consumers will still consent to the processing of their data for OPP purposes (in what is known as the 'privacy paradox'[112]), in particular if the consent request is worded in an engaging way[113], leading them to believe that OPP would never work to their disadvantage[114]. Another possible option for traders would be to have consumers consent to the processing of their personal data for OPP through an OPP browser setting, if this shows technically possible[115]. In any case, for consent to be informed, the EDPB has stressed that data subjects need to be provided with, at least, a minimum set of information elements, including the controller's identity, the types of data which will be collected and used and whether the data shall be used for automated decision-making under Article 22 GDPR[116]. However, providing this information through browser settings does not seem feasible in the current state-of-the-art[117]. Additionally, if traders decide to engage in OPP which falls under Article 22(1) GDPR or if it involves the processing or inferring of sensitive personal data[118], they will need to obtain an "explicit"

---

111 ibid paragraph 86. In a study published in April 2020, Nouwens and others show that only 11,8% of 10.000 analyzed websites in UK complied with the GDPR standards for valid consent for the placement of cookies. See Nouwens M and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020) CHI '20.

112 See F Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017), EDPL 3, 6.

113 The UK DPA has stressed that "it may still be possible to incentivize consent to some extent. There will usually be some benefit to consenting to processing. For example, if joining the retailer's loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who don't sign up does not amount to a detriment for refusal. However, you must be careful not to cross the line and unfairly penalize those who refuse consent." See Information Commissioner's Office, *What is Valid Consent?*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what2, consulted on 21st May 2020.

114 As noted by Vieira Ramos, consumers tend to be overly optimistic, as they normally consider that negative events, such as paying a higher price than other consumers for the same product just because of what they have searched online earlier that week, are more likely to happen to others than to themselves. See M Vieira Ramos, 'Psicologia e Direito do Consumo' (n 45), 361.

115 While the CJEU has clarified that data subjects "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" (notably, if this purpose is OPP), the EDPB, in line with Recital (42) GDPR, has recently stressed that "[browser settings intended to collect consent for data processing] should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers." The CJEU's position seems to be more aligned with Article 6(1)(a) GDPR, however, since consent needs to be granted for specific purposes, not for specific controllers, even if controllers need to be able to demonstrate data subjects have consented to the processing of their data, under article 7(1) GDPR. See Laura Drechsler & Benito Sánchez, 'The Price is (Not) Right' (n 5), 4; Judgement of 14th October 2010, *Deutsche Telekom AG v Bundesrepublik Deutschland*, C-543/09, ECLI:EU:C:2010:603, paragraph 61; and EDPB, *Guidelines 05/2020* (n 113), paragraph 89.

116 See EDPB, *Guidelines 05/2020* (n 113), paragraph 64.

117 See Information Commissioner's Office, *op. cit.* note 105. Even if Recital (66) of the Cookie Directive suggests browser settings as a means of obtaining user consent for the placement of cookies, said option has been scrapped from the latest revised draft of the ePrivacy Regulation Proposal. See Council, DRAFT doc. st9931/20 on ePrivacy, available at <http://downloads2.dodsmonitoring.com/downloads/EU_Monitoring/2020-09-24_Projet_e-privacy_Allemagne.pdf>, consulted on 29 September 2020.

118 The wide catalogue of elements of information protected as special categories of data under Article 9(1) GDPR, whose processing is forbidden unless one of the exceptions in indent (2) applies, deems to prevent data subject discrimination based on their most sensitive personal attributes. This catalogue encompasses characteristics which are not specifically protected under EU secondary anti-discrimination law (see Chapter III, above), such as political opinions, religion health condition and sexual orientation.

consent, which amounts to a higher threshold of accountability[119].

For consent to be informed, in cases involving OPP falling under Article 22(1) – see above –, consumers need to be informed beforehand about the logic behind the pricing algorithm, as well as the significance and the envisaged consequences of OPP.[120] While this does not force traders to explain each individual pricing decision taken by the algorithm to consumers[121], they will need to explore "clear and comprehensive ways to deliver the information to the data subject, for example: the categories of data that have been or will be used in the profiling or [OPP] process; why these categories are considered pertinent[122]; how any profile used in the [OPP] process is built, including any statistics used in the analysis; why this profile is relevant to the [OPP] process; and how it is used for [the pricing decision].[123] Some traders may, however, feel tempted to convey the least possible amount of information to data subjects about these practices, with the justification that their pricing algorithm is protected under their fundamental freedom to conduct a business.[124]

On the "envisaged consequences" element, traders may wish to inform data subjects that the OPP process will lead to the price being reduced or increased up to a maximum of x% of the reference price or when compared to prices paid by other consumers, thus allowing for a conscious decision on whether or not to accept OPP.[125] Once more, traders will struggle with complying with this information duty if they are not fully aware of how the pricing algorithm works. Where the algorithm is developed by a third-party contractor without very precise instructions from the trader, the latter will likely need to ask the former for assistance with complying with GDPR information requirements. Contractors could, however, refuse to provide said assistance for trade secrecy reasons.[126]

As illustrated in this chapter, EU privacy and data protection law does not outright prohibit OPP, but places traders wishing to deploy it at a compliance crossroads. Firstly, the

---

[119] The difference between "express" and "explicit" consent is that the latter "requires a high degree of precision and definiteness in the declaration of consent, as well as a precise description of the purposes of the processing". See Bygrave, *The EU General* (n 99), 377. The EDPB adds that "The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. (…) For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature." See EDPB, *Guidelines 05/2020* (n 113), paragraphs 93 and 94.

[120] See Articles 13(2)(f) and 14(2)(g) GDPR.

[121] Wachter, Mittlestadt and Floridi argue that the wording in the GDPR confers the data subject a right to *ex ante* explanations of [AI] *system functionality* (eg. the system's requirements specification, decision trees, pre-defined models, criteria, and classification structures), not the rationale and circumstances of *specific decisions* taken by the system. In the authors' view, Recital (71) GDPR confers a "non-binding right to an explanation of specific decisions after decision-making occurs". See S Wachter, B Mittelstadt & L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) International Data Privacy Law Vol. 7 No. 2, 82.

[122] On this, Drechsler & Benito Sánchez have claimed that this "could mean (…) that an individual subject to [OPP] receives information on what datasets are considered positively and what datasets are considered negatively for [the price which is presented to him/her]". See Laura Drechsler & Benito Sánchez, 'The Price is (Not) Right' (n 5), 12.

[123] See WP29, *Guidelines on Automated individual decision-making* (n 102), 31.

[124] On how the CJEU has been striking a balance between the controller's freedom to conduct a business and the data subject's fundamental right to data protection, see Judgement of 29th January 2008, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54, paragraphs 62 to 70.

[125] See Information Commissioner's Office and The Alan Turing Institute, *What goes into an explanation?* [2020], available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/what-goes-into-an-explanation/, consulted on 4th June 2020.

[126] See note 17.

distribution of roles and responsibilities between traders and their OPP suppliers with respect to the processing of consumers' data is not clear. Secondly, the processing of consumer data for OPP purposes generally requires prior consent from the data subjects (consumers), which they will possibly not grant if they are properly informed about how OPP works. Thirdly, as data controllers, traders must comply with cumbersome information duties towards consumers who are subject to OPP, which require them to understand how their pricing algorithms work. With DPAs across the EU increasingly focusing on cookie rules enforcement[127] and algorithmic discrimination[128], traders are bound to be taking a careful look into if and how they shall pursue OPP practices.

To top it off, traders deploying pricing algorithms – even those complying with data protection rules and the new Omnibus Directive transparency requirement – will need to ensure their OPP does not constitute a forbidden unfair commercial practice. This is analyzed in the ensuing chapter.

5. OPP as an Unfair Commercial Practice?

The UCPD lays down the rules on commercial practices which, given their unfair, misleading or aggressive nature, traders are not allowed to pursue. Some examples of these restricted practices are "falsely stating that a product will only be available for a very limited time", "presenting rights given to consumers in law as a distinctive feature of the trader's offer" or telling the consumer that "if he does not buy the product or service, the trader's job or livelihood will be in jeopardy"[129]. Although the Omnibus Directive introduced some amendments to the UCPD, these are not directly relevant for addressing OPP's compliance with the UCPD[130].

Although it is true that OPP per se does not seem to constitute an unfair commercial practice, forbidden under the UCPD[131], the EC has highlighted that "personalized pricing/marketing could be combined with unfair commercial practices in breach of the UCPD"[132].

It is possible to envisage how OPP could constitute a misleading commercial practice, under Article 6(1)(d) UCPD[133], notably where the trader, when complying with the novel Omnibus Directive transparency requirement regarding OPP, falsely informs the consumer that the pricing algorithm will always show him lower prices than what the trader would offer in case the pricing algorithm were not used[134]. On whether this particular practice would

---

[127] See Bird&Bird, *The Spanish Data Protection Authority fines Vueling with 30,000 euros for failing to comply with cookie rules*, October 2019, available at https://www.twobirds.com/en/news/articles/2019/spain/la-aepd-ha-impuesto-a-vueling-una-multa-de-30000-euros, consulted on 4th June 2020.

[128] See CNIL, *Algorithmes et discriminations : le Défenseur des droits, avec la CNIL, appelle à une mobilisation collective, 2nd June 2020*, available at https://www.cnil.fr/fr/algorithmes-et-discriminations-le-defenseur-des-droits-avec-la-cnil-appelle-une-mobilisation, consulted on 4th June 2020.

[129] See Annex I of the UCPD.

[130] Nonetheless, the Omnibus Directive does create possibilities for consumers to access "proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract." The right of having the price for a good or service reduced after becoming aware that the price algorithm worked to their disadvantage (contrarily to what traders may advertise), could serve as a useful tool for consumers targeted by OPP. See Article 4(5) Omnibus Directive.

[131] See Sears, 'The Limits of' (n 5), 16.

[132] See EC, *Staff Working Document* (n 20), 134.

[133] Which forbids the trader to inform the consumer in a deceitful (or likely deceitful) manner about the product's or service's price or the manner in which the price is calculated.

[134] See Authority for Consumers and Markets Authority, *Guidelines on the Protection of the online consumer* (n 82), 25.

likely deceive the average consumer[135] and could cause him to take a transactional decision[136] that he/she would not have taken otherwise, there are good arguments to support a positive answer: given that the average consumer is price-oriented and not really aware of how OPP works[137], any indication given by the trader that he/she will be always granted a discount in case he/she accepts OPP is likely to lead the consumer to accept OPP and even to purchase products and services from the trader that he/she would otherwise not.

OPP could also be associated with a misleading omission under Article 7(1) or (2) UCPD. If a trader does not inform the consumer that the price he/she is being offered in the online shop has been calculated by a pricing algorithm (in breach of the new transparency duty stemming from the Omnibus Directive), or does so in an "unclear, unintelligible, ambiguous or untimely manner", this should be regarded as a misleading omission[138]. In fact, since the enactment of the Omnibus Directive – making the provision of information about OPP mandatory for traders – this should be considered "material information" for the purposes of those provisions of the UCPD, which needs to be given to consumers to allow them to take a conscious decision about whether or not to engage with traders deploying pricing algorithms[139]. This is so even today, before the Omnibus Directive has been transposed by the EU Member-State where the consumer has his/her habitual residence[140] or before 28th November 2021 (the deadline for transposing the Omnibus Directive[141]), as – in line with CJEU case law – national law transposing the UCPD should be read under the light and in accordance with Directives (such as the Omnibus Directive) which lay down a general principle of EU law (like consumer protection), even before their transposition deadline has elapsed[142].

---

135 I.e., one "who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors". See Recital (18) UCPD.

136 As clarified by the EC, a 'transactional decision', for the purposes of Article 6(1) UCPD, does not necessarily mean the decision of purchasing or not purchasing a product or service, but may also be a pre-purchase or post-purchase decision, such as a decision to click through a webpage as a result of a commercial offer. See EC, *Staff Working Document* (n 20), 33-35.

137 See Ipsos, London Economics & Deloitte, *Report for DG JUST* (n 12), 103: "The self-reported awareness about *online personalised pricing* was on average quite lower than the self-reported awareness about online targeted adverts and personalised ranking of offers. Across the EU28, slightly more than four in ten (44%) of respondents reported to understand or have some understanding of how personalised pricing used by online firms works. In contrast, nearly 3 out of 10 (29% of) respondents mentioned that they hadn't heard of it up until now (versus only 8% and 11% for targeted advertising and personalised ranking of offers, respectively).

138 In order to avoid this, traders may wish to follow the WP29 information-provision checklist about automated decision-making, when delivering information to consumers about OPP. See Chapter IV and WP29, *Guidelines on Automated individual decision-making* (n 102), 31.

139 Even where the pricing algorithm would normally benefit the consumer at stake, by offering him/her a lower price than to most other consumers. See Miller, 'What Do We Worry' (n 1), 85; and Priester, Robbert and Roth, 'A Special Price' (n 3), 104 and 105.

140 Under the Rome I Regulation, this should be, as a rule, the law applicable to contracts concluded between traders and consumers. See Article 6(1) of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

141 Article 7(1) Omnibus Directive.

142 In Mangold, the CJEU awarded horizontal indirect effect to a Directive which deemed to ensure equal treatment (in particular, non-discrimination based on age) in the field of employment and occupation, even before the deadline for transposal of the Directive had elapsed. On that occasion, the Court held that non-discrimination on grounds of age "must be regarded as a general principle of [EU] law" and, thus, its observance "cannot as such be conditional upon the expiry of the period allowed the Member States for the transposition of a directive intended to lay down a general framework for combating discrimination on the grounds of age". On a generous reading of said judgement, one may argue that Article 4(4)(ii) of the Omnibus Directive intends to lay down a provision for ensuring consumer protection vis-à-vis OPP, and that consumer protection is also a general principle of EU Law, under Article 6(1) and (3) of the Treaty on European Union – as it is enshrined in Article 38 CFREU –, and, thus, the same rationale could apply to interpreting current Member-State law

Moreover, the Dutch Authority for Consumers and Markets (ACM) has recently raised the possibility of certain OPP strategies being considered as aggressive commercial practices, for the purposes of Article 8 UCPD. As an example, the ACM mentions a trader who misuses its "knowledge of a consumer's vulnerable circumstances [eg. acquired through insights provided by data brokers or by cookies tracking the consumer's browsing through fast, easy and high-interest credit providers' websites], possibly by offering products on instalment credit to financially vulnerable and/or indebted consumers"[143].

Even if certain OPP practices do not qualify as misleading actions or omissions, nor as aggressive commercial practices, they may still be considered as unfair commercial practices under the Article 5(2) UCPD 'safety net'. However, in this case, OPP practices would need to be assessed against the requirements of professional diligence, i.e., "the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity"[144]. Additionally, for it to be forbidden, OPP would need to, in a given case, be liable to materially distort the economic behavior of the "average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers"[145] Although this latter criterion seems fitting for assessing the fairness of third-degree online price discrimination practices, the same cannot be said of OPP, which is specifically targeted to individual consumers, and not to groups of consumers. Therefore, the "average consumer" criterion seems inadequate to evaluate the fairness of a given OPP practice, given the nature of OPP. In this regard, special mention to Article 5(3) UCPD should also be made. The provision reads that "Commercial practices which are likely to materially distort the economic behavior only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity[146] in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group". In cases of third-degree online price discrimination where the trader uses a pricing algorithm to target children with predatory prices, for instance, it would be more likely that the trader could foresee that this pricing strategy would impact those vulnerable consumers in a manner incompatible with Article 5 UCPD. But, once again, for cases of OPP, it would be more appropriate to have the trader consider the particular vulnerability (eg. an alcohol addiction or economic exposure inferred from repeated detection of the consumer's GPS location at a given liquor store or low-income neighborhood) of the specific consumers targeted with personalized prices, taking into account the information at its disposal about said consumers. All in all, the "average consumer" criterion appears outdated when assessing the fairness of OPP

transposing the UCPD in conformity with the new OPP-related transparency requirement. Judgement of 22nd November 2005, *Werner Mangold v Rüdiger Helm*, C-144/04, ECLI:EU:C:2005:709, paragraphs 75 and 76. See also Judgement of 14th May 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*, 4-73, ECLI:EU:C:1974:51, paragraph 13; and Judgement of 26th February 2013, *Åkerberg Fransson*, C-617/10 ECLI:EU:C:2013:105, paragraphs 20 and 21.

[143] See Authority for Consumers and Markets Authority, *Guidelines on the Protection of the online consumer* (n 82), 25.

[144] Article 2(h) UCPD. It would likely be against professional diligence for traders to not inform consumers about OPP, thereby significantly impairing their freedom of choice of not engaging with traders deploying pricing algorithms. See Judgement of 26th October 2016, *Canal Digital Danmark A/S*, C-611/14, ECLI:EU:C:2016:800, paragraph 55.

[145] Article 5(2)(b) UCPD.

[146] The vulnerability factors outlined in Article 5(3) may not be exhaustive, given the wording of Recital (19) UCPD, which uses the expression "such as". According to Vieira Ramos, "situations such as [the consumer's] socio-economic condition, lack of experience, knowledge or habilitations also constitute important sources of vulnerability". See M Vieira Ramos, 'Psicologia e Direito do Consumo' (n 45), 449.

under Article 5 UCPD, which hints at the need of replacing or complementing it with a more suiting one.

Before presenting the paper's conclusions, it should be stressed that the application of the UCPD rules to OPP practices remains mostly untested by national courts and the CJEU, and that further clarity as to how the Directive's concepts apply to this relatively new practice is needed.

Conclusions.

As this paper tried to show, no matter how much consumers seem to dislike OPP, this practice is not outright forbidden under EU law and does not seem to be going away anytime soon[147].

Online price discrimination grounded on consumers' specially protected characteristics (such as gender, race, nationality or place of residence), in turn, is prohibited under EU certain (limited) anti-discrimination instruments, unless traders can provide objective justification for price differentiation based on said features. The burden of proof about the existence of discrimination, however, lies with the consumer/plaintiff, which may ultimately render these tools ineffective when a complex pricing algorithm decides considering various personal attributes which are fed to it about consumers.

The new transparency requirement brought by the Omnibus Directive in relation to OPP will shed light on this practice for consumers, which ought to be informed, in a clear and prominent manner and directly before clicking 'buy', about whether the price they are seeing when buying online has been tailored to their online profile(s) by a pricing algorithm. This warning must be written in a plain and intelligible language, every time a personalized price is offered, thus allowing the consumer to understand how OPP shall work in each case it is used. Further guidance from consumer protection bodies is needed to understand what level of detail of information should be conveyed to consumers in OPP tags. The upcoming EU instrument on AI could also consider pricing algorithms as "high-risk" AI applications, thus mandating enhanced transparency requirements in this regard towards consumers and regulators.[148]

European privacy and data protection places heavy incumbrances on traders wishing to collect and further process consumer data for OPP purposes. In general, this requires traders to obtain prior free and express consent from consumers, and to inform them about how the pricing algorithm will use their data to target them with personalized prices. Trade secret justifications may impede traders from receiving assistance from contractually engaged data brokers or data analytics companies with complying with said obligations, as well as from giving consumers meaningful information about the consequences OPP entails for their legal or financial interests.

Lastly, traders supplying false, incomplete or untimely information to consumers about OPP could face consequences from a consumer law perspective – notably, by having to offer a price reduction to consumers whose price was personalized –, as those may amount to misleading actions or omissions under the UCPD. The "average consumer" criterion seems to be of little use for assessing whether a commercial practice such as OPP – which, by its nature, is addressed to a specific consumer, and not to larger or narrower groups of consumers – is unfair for the purposes of the UCPD.

---

[147] O Bar-Gill, 'Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions' (2018) The University of Chicago Law Review, available at https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3184533_code837010.pdf?abstractid=3184533&mirid=1, consulted on 4th June 2020, Section I.A.

[148] EC, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final [2020].

Enforcement of and further guidance on the rules applicable to OPP by Equality Bodies[149], DPAs and Consumer Protection Authorities is expected and needed to understand if traders deploying pricing algorithms will be subject to legal scrutiny as tight as the one being exerted by scholars. But also to see whether regulators and courts will award it the same "tolerance" as people tend to concede when they realize they have paid a different price than other consumers due to their recent whereabouts or Facebook likes.

[149] "The European Network of Equality Bodies (Equinet) promotes equality in Europe by supporting and enabling the work of national equality bodies, bringing together 46 organisations from 34 European countries. The EU equal treatment legislation requires Member States to set up an equality body to provide independent assistance to victims of discrimination. Most Member States have implemented this requirement, either by designating an existing institution or by setting up a new body to carry out the tasks assigned by the new legislation. However, no specific guidelines exist for Member States on how these bodies should operate. So far, European antidiscrimination law only requires that equality bodies are set up in the fields of race, ethnic origin and gender. Many countries have bodies that deal with other grounds of discrimination as well." See FRA, *Handbook* (n 79), 25.