Belgium

Louis Hoffreumon and Benjamin Docquir

Louis Hoffreumon, Osborne Clarke, Brussels
E-mail: Louis.Hoffreumon@osborneclarke.com

Benjamin Docquir, Osborne Clarke, Brussels
E-mail : Benjamin.Docquir@osborneclarke.com

1. Introduction

The recent years have seen many new forms of marketing practices from businesses that target consumers with an increasing use of AI and other computational or profiling technologies. Not only marketing as such is concerned by these practices, but also advertising, promotions, pricing, and also entering into an agreement with the consumer, with the final objective to sell goods or procure a service.

This shift towards an increasingly virtualised environment raises questions regarding the appropriateness of the current legal protections and remedies offered to the consumer, under Belgian and EU law, as the target of such practices, a contractual counterparty and an individual whose personal data is processed by a data controller.

In this new paradigm, practitioners are facing a growing interaction between the laws protecting consumers (trade practices, consumer contracts, e-commerce and unfair competition), mostly issued from EU directives (as further described hereunder), and the rules on the protection of privacy, including the GDPR, adopted in 2016 . A GDPR consent form that must comply with the Unfair Terms Directive[1] when obtaining consent from a data subject[2] appears as the most obvious and well-known example.

Moreover, when commenting on the New Deal for Consumers, the European Data Protection Supervisor ("EDPS") appreciated that both consumer and data protection law shared common goals of redressing imbalances of informational and market power, and, together with competition law, they needed to work in a consistent manner to ensure that people are treated fairly.[3] We will use this common thread throughout this contribution.

Under Belgium domestic law, there currently is no unique legislation dealing specifically with this new paradigm. Consequently, at the time of this contribution, such issues continue to be approached according to unfair competition and economic law rules with regards to consumer rights, and according to the GDPR and its domestic implementations when regarding the processing of the same consumers' personal data, each being dealt with by separate regulators.[4]

In this contribution, we provide a description of the current Belgian legal landscape on advertising and marketing (Section 2), and discuss two currently debated topics: first, this contribution questions if the current scope of legislation on "commercial communication" and "identifiability" could be improved to address new forms of marketing and advertising (Section 3). Second, we assess the interactions between consumer and privacy laws illustrated by the concept of consumer personalisation in an online environment, whether or not using automated means such as AI (Section 4).

---

[1] Council Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts, OJ 1993, L 95, p. 29.
[2] GDPR, Recital 42.
[3] Opinion 8/2018 of the EDPS, on the legislative package "a New Deal for Consumers", available at: https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf, pts 6-7, p. 8. The same idea can be found in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European Strategy for data, COM(2020) 66 final, 19 February, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN. Accessed 5 March 2021.
[4] Namely, the Belgian ministry of economy, for the most part, regarding compliance by enterprises with consumer rights set out under Book VI of the Code of Economic Law, in Belgium, and the Belgian Data Protection Authority ("BDPA"), concerning issues related to privacy and consumers' personal data.

We will use the terminology in force under Belgian law and speak of "enterprise" when referring to a trader (as defined under the EU directives, being a 'professional' targeting consumers) or data controller (the same trader acting as advertiser, advertising network, data source or collecting the consumer's personal data for further processing in order to send him or her personalised advertisings and, subsequently, goods and/or services). On the other hand, we will refer to "consumer" when talking about the other party to that relationship, the consumer receiving the ads and purchasing the goods and/or services at the end of the chain, being also the data subject under the GDPR whose data is collected and processed.

2. The Belgian Legislative Landscape

2.1 Unfair Commercial Practices

2.1.1 General Legislation

The relevant legislation implementing (i) the Advertising Directive,[5] (ii) the Unfair Commercial Practices Directive, (iii) the Unfair Terms Directive, (iv) the Directive on electronic commerce, (v) some provisions of the e-Privacy Directive[6] and (vi) the Consumer Rights Directive[7] is contained in Books VI ("Consumer Law and Trade Practices") and XII ("Digital Economy") of the Belgian Code of Economic Law ("CEL").[8]

First, Book VI CEL deals with consumer information in the market,[9] unfair commercial practices [10] (defined as "any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a business, directly connected with the promotion, sale or supply of a product to consumers"), [11] and with B2C contracts.[12] [13]

A commercial practice can be deemed unfair, and may be subject to civil or criminal sanctions, following the widely accepted "three-time reasoning" by Belgian scholars and practitioners under Article 5 of the Unfair Commercial Practices Directive and their Belgian counterpart: the fairness of a practice is first considered under a general norm : a commercial practice is unfair if contrary to the requirements of professional diligence and influences the economic behaviour of a consumer. Then, some practices will be deemed unfair under a "semi-general" norm if they are misleading or aggressive. Finally, specific practices are deemed unfair in all circumstances if they are contained in a "black-list".[14] As practitioners ourselves, we prefer a dynamic and risk-oriented approach, which is more appropriate in terms of legal design, where the order of such reasoning is reversed as described below.

First, a practice will be tested against the "blacklist" of specific commercial practices deemed unfair in all circumstances for consumers (and therefore forbidden) whether because they are considered misleading or aggressive.[15]

[5] Directive 2006/114 of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, OJ, 2006, L 376, p. 21.
[6] Directive 2002/58 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 (Directive on privacy and electronic communications), OJ 2002, L 201, p. 37.
[7] Directive 2011/83 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 of the European Parliament and of the Council and repealing Council Directive 85/577 and Directive 97/7 of the European Parliament and of the Council.
[8] Act of 28 February 2013 creating the Code of Economic Law, Belgian Official Gazette, 28 February 2013, p. 19975.
[9] Articles VI.1/1 to VI. 36 CEL.
[10] Articles VI.92 to VI.117 CEL.
[11] Article I.8, 23° CEL.
[12] Articles VI.37 to VI.91 CEL.
[13] These provisions will evolve in the future following the upcoming implementation under Belgian law of the contents of the Omnibus Directive and the Digital Content Directive, both adopted in the framework of the New Deal for Consumers, and which will be considered later in this contribution where relevant.
[14] Annex I of the Unfair Commercial Practices Directive.
[15] Respectively articles VI.100 and VI.103 CEL, implementing Annex I of the Unfair Commercial Trade Practices Directive.

At a second stage, if the practice is not captured by this blacklist, one needs to assess if it falls under the "semi-general norm". Under this second set of rules, a practice is deemed unfair if it is misleading[16] or aggressive[17] and has as effect to cause the consumer to take a transactional decision[18] that he or she would not have taken otherwise.

A practice will be considered misleading when it contains false information or, where no false information is conveyed, if it is deceitful or likely to deceive the average consumer regarding some of its elements, including the main characteristics of the product, endorsements, prices and methods of price calculation, or the identity of the business. Parasitic competition or the omission of material information[19] from the consumer are other examples of misleading commercial practices.

A commercial practice will be considered as aggressive if, in its factual context, taking into account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product, causing the consumer to take a transactional decision that he would not have taken otherwise.[20]

If the envisaged practice can neither be deemed misleading nor aggressive, a third stage will consist in assessing whether the enterprise complies with "general norm" for unfair commercial practices. Under this norm, a commercial practice is unfair if it is both contrary to the requirements of professional diligence and materially distorts or is likely to materially distort the economic behaviour of the average consumer whom it reaches or to whom it is addressed with regard to the product, or of the average member of the group when a trade practice is directed to a particular group of consumers.[21] In the latter case, the enterprise must assess the practice from the perspective of the average member of a clearly identifiable group of consumers that is particularly vulnerable because of mental or physical infirmity, age or credulity.

Next to the commercial practices directed to consumers, Book VI CEL contains rules applicable to commercial practices detrimental to other businesses. While not envisaged in this contribution, a central provision in that regard is Article VI.104 forbidding any commercial practice from a business that is detrimental to the professional interests of one or several businesses. Under this rule, unanimous case-law considers that either a breach of any legislation or adopting behaviour contrary to the requirements of professional diligence were sufficient to establish the existence of such forbidden practice.[22] As a result, practices that infringe upon consumers' rights to privacy or otherwise do not comply with statutory rules on processing of personal data, recording of, or access to, electronic communications data, can justify an application for injunctions or cease-and-desist measures on the part of a competing enterprise.

---

[16] Article VI.97 to 99 CEL (misleading commercial practices towards consumers); article VI.105 and 105/1 CEL (misleading commercial practices towards enterprises).

[17] Article VI.101-102 CEL (aggressive commercial practices towards consumers); article VI.109/1 to 109/3 CEL (aggressive commercial practices towards enterprises).

[18] Article I.8, 28° CEL. A "transactional decision" means any decision concerning whether, how and on what terms to, for the consumer, purchase, make, retain or dispose of a product or proceeds to a payment in whole or in part for such product, or exercises a right in relation thereto.

[19] Such material information is listed under Article VI.99, §4 CEL and include (1°) the main characteristics of the product, in the appropriate measure and taking into account the means of communication and the product concerned, (2°) the geographic address and the trader's identity and, if applicable the geographical address and the identity of the enterprise on which account the trader is acting; (3°) the price (all taxes included), or, when it can be calculated in advance, the way that the price is calculated together with, if applicable, all additional transport, shipping and delivery costs or, when these costs cannot be calculated in advance, the mention that these costs can be charged to the consumer; (4°) the process for payment, delivery, processing complaints, if they are different from professional standards; (5°) the existence or not of a withdrawal right. Under article VI.99, §5 CEL, are also considered material all mandatory information in relation with commercial communication, under the directives listed under Annex II of the Unfair Commercial Practices Directive, as well as other mentioned European legislation.

[20] For completeness, article VI.102 CEL set outs the elements to take into account to assess the presence of harassment, coercion, including the use of physical force, or undue influence: (1°) its timing, location, nature or persistence; (2°) the use of threatening or abusive language or behaviour; (3°) the exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgment, of which the trader is aware, to influence the consumer's decision with regard to the product; (4°) any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader; (5°) any threat to take any action that cannot legally be taken.

[21] Article VI.93 CEL.

[22] For a complete overview of the principles based on this article, see J. Stuyck and B. Keirsbilck, Artikel VI.104 WER: oneerlijke mededinging in J. Stuyck, B. Keirsbilck, Handels- en economisch recht, Serie 'Beginselen van het Belgisch Privaatrecht", n°14, Kluwer, Malines, 2019, pp. 204-302.

Read together, it appears that the general norm has the potential for a broad application and can be of use to qualify any practice in breach of the law as an unfair commercial practice.

Two other sets of rules under this Book are worth mentioning. First, Article VI.17 CEL describes the applicable rules to comparative advertising, which are similar to the ones contained under Article 4 of the Advertising Directive. Second, the recent so-called "B2B Act"[23] introduces a similar set of rules in relation with commercial practices in a B2B context.

Book XII CEL, under its Title I,[24] deals with advertising and marketing when they are provided by means of information society services,[25] and implements, *inter alia*, the transparency and information obligations contained herein (Articles XII.6 and 7), together with technical provisions on agreements,[26] the identifiability requirements for advertising and promotions (Article XII.12), the (opt-in) rules on electronic marketing by e-mail (Articles XII.13 and 14) and the rules on editorial responsibility applicable to intermediaries (Articles XII.17 to XII.20).

2.1.2 Specific Legislation

In relation to advertising and marketing, and in addition to the general legislation, some sectors or products remained governed by specific legislation at Belgian or EU level (among others gambling,[27] medicines, [28] alcohol and tobacco, [29] food[30] and cosmetics[31]).

The rules applicable to advertising in audio-visual media services, as defined under the AVMS Directive,[32] have been implemented at the regional level and are subject to three different regional decrees.[33] Stricter rules apply to

[23] Law of 4 April 2019 amending the Code of Economic Law regarding abuses of economic dependence, abusive clauses and unfair market practices between undertakings, Belgian Official Gazette, 24 May 2019, p. 50066. This law is intended to protect SMEs against commercial practices that are similar to those used for consumers, and used by bigger and international businesses. According to the drafters of the Act, SMEs should enjoy the same protection as consumers. See Draft Act amending the Code of Economic Law regarding abuse of a significant dominant position, 13 November 2015, Doc. Parl. Ch., 2015-2016, n°54-1451/1, p. 6.

[24] For completeness, Book XII CEL contains a Book II in relation with the rules applicable to trust services as provided under the eIDAS Regulation (Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93, OJ, 2014, p. 73).

[25] The Directive on electronic commerce refers to the definition of "information society services" given under Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ, 2015, L 241, p. 1.

[26] Articles XII.8 to 11, 15 and 16 CEL.

[27] Act of 7 May 1999 on Gambling, Betting, Gambling Establishments and Gambler Protection, Belgian Official Gazette, 30 December 1999, p. 50040 (and subsequent amendments) and the Royal Decree of 25 October 2018 on Modalities for the Operation of Games of Chance and Betting Operated by Means of Information Society Instruments, Belgian Official Gazette, 31 October 2018, p. 82744.

[28] Article 9 of the Act of 25 March 1964 on Medicines, Belgian Official Gazette, 17 April 1964, p. 4206, and its subsequent executing decrees. This Law also implemented the rules set out under Directive 2001/83.

[29] Act of 24 January 1977 on Consumer Health Protection in relation with Foodstuffs and other Products, Belgian Official State Gazette, 8 April 1977, Article 7.

[30] See, among others, article 16 of Regulation No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, OJ 2002, L 31, p. 1; Regulation 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, OJ 2011, L 304, p. 18; and Regulation 1924/2006 of the European Parliament and of the Council of 20 December 2006 on nutrition and health claims made on foods, OJ 2006, L 404, p. 9. For the aspects not covered by European legislation, the abovementioned Act of 27 January 1977 and its executing decrees remain applicable.

[31] Article 20 of Regulation No 1223/2009 of the European Parliament and of the Council of 30 November 2009 on cosmetic products, OJ 2009, L 342, p.59.

[32] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, OJ 2010, L 95, p. 1. Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018, amending the AVMS Directive, has recently been implemented under Belgian law. See footnote n°36.

[33] In Belgium, audio-visual media services are regulated at "communities" level (Belgian territories divided depending on language and culture), resulting in three different set of legislations implementing the AVMS directive, pertaining to the Dutch-speaking community (*Decreet van 27 maart 2009 betreffende radio-omroep en televisie,* Belgian Official Gazette, 30 April 2009, p. 34470, and the amending decree of 19 March 2021 implementing the new AVMS Directive, Belgian Official Gazette, 29 April 2021, p. 40930), French-speaking community (*Décret coordonné du 26 mars 2009 sur les services de médias audiovisuels,* Belgian Official Gazette, 24 July 2009, p. 50609, now replaced by the *Décret du 4 février 2021 relatif aux services de médias audiovisuels et de services de partage de vidéos*, Belgian Official Gazette, p. 29036), and German-speaking community (*Dekret vom 27. Juni 2005 über den Rundfunk und die Kinovorstellungen*, Belgian Official Gazette, 6 September 2005, p. 38869, now replaced by the *Dekret vom 1. März 2021 über die Mediendienste und die Kinovorstellungen*, Belgian Official Gazette, 12 April 2021, p. 32156). Moreover, media falling under the scope of this Directive are governed by three different regulators also operating at community level. Audio-visual media services not attached to any of these region remain governed by a supplementary federal law, the Law of 5 May 2017 relating to the audiovisual media services in the bilingual region of Brussels-Capital, Belgian Official Gazette, 23 May 2017, p. 58970.

advertising and its identifiability but only as far as it is conveyed on specific "audio-visual" media and, since 2018, on "video-sharing platform services" falling under the scope of the AVMS Directive. This may create issues for the provider of online services who needs to determine if its service falls under the scope of these rules and then needs to assess whether it needs to remind its users of them, or in some cases take an active part in monitoring their compliance.

2.1.3 Self-Regulation

Next to State legislation, the legal framework of advertising is characterised by self-regulation, supervised in Belgium by an independent non-governmental body, the BEJA (*Jury d'éthique publicitaire*; *Ethische Jury voor Ethische Praktijken inzake Reclame*).[34]

The BEJA is a non-profit association that is vested with the competence to render decisions on the conformity of an advertisement with legal and ethical rules protecting the consumer, either based on mandatory legislation or on self-regulatory codes (being primarily the ICC Marketing and Advertising Communications Code (ICC Code) and guidelines and rules adopted based on it).[35] These decisions are not legally enforceable and cannot be subject to a fine or specific sanctions.

Here again the scope of this self-regulation is limited to specific media (television, cinema, radio, but also "digital" medias: an advertiser's own website, pop-ups, search results, in-app advertising or "advergaming"). Questions in relation to other commercial practices, IP, or aspects of direct marketing that do not relate to advertising *strico sensu* (including databases, processing of personal data, behavioural advertising) fall outside of its scope.[36]

2.2 Privacy and Personal Data

The GDPR is fully applicable under Belgian law and is completed by specific rules under the Data Protection Act[37] and the Act creating the (Belgian) Data Protection Authority ("BDPA").[38] For instance, Article 7 of the Data Protection Act implements Article 8 GDPR and sets the age at which an underage data subject is able to consent to the processing of its personal data without intervention from its legal guardians to be thirteen or more.

The BDPA, when issuing decisions, is required to take into account not only the rights and freedoms of individuals in relation with processing and circulation of their personal data, but also the country's consumer protection policy.[39] Building on this obligation, the BDPA made direct marketing, a practice having an impact on consumers directly, one of its priority sectors for the upcoming five years and further scrutiny is to be expected on the enterprises processing personal data for these purposes.[40]

---

[34] As self-regulatory advertising body, the BEJA is also a member of the European Advertising Standards Alliance (EASA).

[35] Article 1 of the BEJA's international regulations as at 1 January 2020, hereafter the "BEJA Regulations" (Consulted on 28 May 2020). Available (in French) at: https://www.jep.be/sites/default/files/inline-media/reglement_jep_fr_-_2020_cc.pdf. Axamples of self-regulatory codes are the Advertising Code for food products, issued with the Food Industry Federation, available at: https://www.jep.be/sites/default/files/rule_reccommendation/fevia_fr.pdf (the "FEVIA Code"); the Convention on advertising and marketing of alcoholic beverages of 25 January 2013, amended on 2 September 2019, available at: https://www.jep.be/sites/default/files/rule_reccommendation/convention_alcool_-_fr_-_2019.pdf; the Advertising Code for advertising and marketing of cosmetic products, revised on May 2020, available at: https://www.jep.be/sites/default/files/rule_reccommendation/code_publicite_produits_cosmetiques_detic_2020.pdf; Code of ethical and responsible advertising by the national lottery, available at: https://www.jep.be/sites/default/files/rule_reccommendation/code_voor_ethische_reclame_fr.pdf. Accessed 10 September 2021.

[36] A complete list of the scope of action of the BEJA is set under article 2 of the BEJA Regulations.

[37] Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, Belgian Official Gazette, 5 September 2018, p. 68616.

[38] Act of 3 December 2017 creating the BDPA, Belgian Official Gazette, 10 January 2018, p. 989. The BDPA has a dedicated website: https://www.dataprotectionauthority.be (for the English version).

[39] Article 52, §1 of the Act creating the BDPA.

[40] See Strategy Plan of the BDPA, p. 23, available (in French or Dutch) at https://www.autoriteprotectiondonnees.be/publications/plan-strategique-2020-2025.pdf. Accessed 12 January 2021.

Singularly, the rules applicable to cookies, implementing Articles 5 and 6 of the e-Privacy Directive, are contained in a separate legislation under Article 129 of the Belgian Electronic Communications Act.[41] However, this Article clearly links cookies to compliance with privacy legislation.[42]

While not binding, the (endorsed) opinions and guidelines issued by the Article 29 Working Party, now the EPDB, together with the recommendations issued by the BDPA remain a useful tool for providing a comprehensive interpretation of some key notions under the GDPR and related legislation. Recently, the BDPA has issued a Recommandation on Direct Marketing[43] inspired by various EDPB guidelines.

2.3 AI

AI is not regulated by specific Belgian legislation, although scholars opine that the existing rules on contract law, next to those on consumer and privacy laws, should apply to the use of AI, subject to a few specific adaptations.[44]

The need to amend the existing legislation, or to adopt a specific text with regards to AI has also been discussed at length at the EU level, taking into account the fact that some specific features of AI (such as the opacity of its functioning) can make the application and enforcement of existing legislations more difficult. [45] At the date of this contribution, the EU Parliament has issued a first proposal regulation in relation to AI liability,[46] providing a first tangible legal initiative on the matter.

3. Identifiability and the Precise Scope of Advertising Laws

Advertising is no longer the reserved playing field for "for profit" actors, selling goods or services, and this raises the question whether "non-commercial" advertising should also be approached by the law. Also, the development of new forms of marketing challenges the identifiability requirement in an environment where new technologies evolve faster than the law.

3.1 Non-Commercial Advertising

Book VI and Book XII CEL each have their own definition of "advertising" that cover communications with the direct or indirect purposes of promoting goods or services. Moreover, under Book XII CEL the communication can also be made to promote the image "of a company, organisation or person having a commercial, industrial or regulated activity".[47] The latter results from the implementation of the definition contained in the Directive on electronic commerce.

Information giving access to the activities of an undertaking or natural person (such as domain name or e-mail address), and independently developed communications (among others, unpaid communications) are excluded from this definition, whereas the CJEU ruled that advertising could also include metatags and domain names when used together and referring to products, services or the commercial name of a company. [48]

---

[41] Act of 13 June 2005 on Electronic Communications, Belgian Official Gazette, 20 June 2005, p. 28070.
[42] Article 129 of the Electronic Communications Act refers to both the information of the consumer, and his or her consent, having to comply with the previous Belgian Privacy Act, which must be read as referring to the GDPR.
[43] BDPA, Recommendation 01/2020 of 17 January 2020 in relation with processing of personal data for direct marketing purposes. Available (in French) at https://autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf. Accessed on on 5 May 2020.
[44] See for instance H. Jacquemin and J.-B. Hubin, L'intelligence artificielle et le droit, Collection du Crids, 2017, Brussels, Larcier Y. Poullet, le RGPD face aux défis de l'intelligence artificielle, Collection du Crids, 2020, Brussels, Larcier; C. Vanleenhove and J. De Bruyne, Artificial Intelligence and the Law, Collection Centrum voor Verbintenissenrecht, 2021, Brussels, Intersentia.
[45] European Commission White Paper on Artificial Intelligence - A European approach to excellence and trust, 19 February 2020, p. 10. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Accessed 10 May 2020.
[46] Proposal for a Regulation on the liability for the operation of Artificial Intelligence-systems, contained in the European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html. Consulted 25 November 2020.
[47] In this interpretation, Book XII CEL contains rules that will come on top of those set out under Book VI when an ad or commercial communication is provided with the use of information society services.
[48] CJEU, 11 July 2013, case C-657/11, *Belgian Electronic Sorting Technology*, ECLI:EU:C:2013:516. However, the court confirms that the registration of a domain name, as such, is not encompassed by this definition. See also A. Bochon, To be a communication or not to be: the influence of IT innovation on the material scope of EU advertising law, R.E.D.C., 2014/25, p. 289-308.

The practice has shown that both definitions tend to be used indistinctively by the courts, and their practical differences due to the way they are interpreted seem to be of little relevance. [49]

These definitions, delineating the scope of application of Book VI and/or XII CEL, contain the requirement that the communication originates from an organisation or company having a lucrative purpose consisting in the provision of goods, services, or their own image. Consequently, "non-profit" advertising, such as communications from political candidates or parties, religious or philosophical associations remain out of the scope of these rules and the consumers do not enjoy protection as to their misleading or aggressive character. However, specific sanctions under criminal law could apply as this practice could constitute offenses such as harassment, proselytising, or breach of electoral laws.[50]

The same idea is found in the AVMS Directive[51] which defines audio-visual commercial communication as images (with or without sound) designed to promote directly or indirectly, the goods, services or image of a natural or legal person pursuing an economic activity qualifying as a service under the TFEU.[52]

The exclusion of non-commercial communication from these rules can be put into question due to the general use of social media by all stakeholders, notably the development of promotional communication of political parties or non-profit associations, that could also convey misleading or aggressive messages. Among many examples, we mention here the increasing appearance of fake-news or unchecked facts used to support a political opinion or comment on the efficiency of vaccines or the actual effects of a pandemic, as well as the use of specific technologies, such as deep-fakes or other sort of sophisticated montages that a recipient would be unable to identify as being "promotional" communication.

This exclusion can raise concerns since these non-commercial forms of advertising could constitute a threat for individuals far beyond their consumer rights: one can wonder how someone can safeguard their freedom of expression, to vote or of religion if they are unknowingly influenced towards waiving some of their personal rights, adopting specific voting decisions or opinions that they would not make in the absence of the "non-commercial" practice at stake.

A reflection should be led at legislative level to consider an extension of the rules applicable to fair commercial practices to other forms of promotional practices that do not have as a main goal the sales of goods or services, and taking into account their specific nature. Building on the definition of the "material distortion of a consumer's economic behaviour"[53] we can think, for instance, of alternative criteria to determine how a non-commercial practice will have an influence on a consumer's decision, which for non-commercial practices will not be animated by economic, but rather "societal" purposes. One can imagine a definition such as "any decision taken by a recipient concerning whether, how and on what terms to make a decision impacting their individual rights and society, to waive or restrict their own freedoms or those of others".

Under privacy laws, this issue is less likely to arise when a similar communication is realised following the processing of personal data. In that case, the communication will qualify as "direct marketing" subject to the requirements of the GDPR, and enjoy a broader understanding that the BDPA defined as "[a]ny communication, whether solicited or unsolicited, aimed at promoting an organisation or an individual, services, products, whether paid or free, as well as brands or ideas, communicated by an organisation or an individual acting for commercial purposes or not, directly to one of more natural persons in a private or professional framework, by any means, and involving processing of personal data".[54]

---

[49] As reported in J. Vandendriessche, Elektronische handel – reclame online in Praktijkboek Recht en ICT, 2015, Bruges, Vanden Broele, p. 19.
[50] See on this subject F. Coppens, Le spamming politique : affaire de harcèlement, de prospection et de traitement de données à caractère personnel?, Rev. dr. pén. Entr., 2010/4, p. 321-330.
[51] For a detailed analysis of the new rules introduced by the new AVMS Directive, see also P. Vlacke, N. Feci and V. Verdoodt, Herziening van de Richtlijn Audiovisuele Mediadiensten: Over Porsches en ezelwagens in tijden van convergentie, A&M, 2018-201, n°2,p. 218-235.
[52] Article 1 (1) (h) of the AVMS Directive. See also Recital 21 AVMS Directive where reference is made, when referring to an economic activity, to the definition of "services" as defined under the TFEU, art. 57: "*Services shall be considered to be "services" within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are no governed by the provisions relating to freedom of movement for goods, capital and persons. "Services" shall in particular include: (a) activities of an industrial character; (b) activities of a commercial character; (c) activities of craftsmen; (d) activities f the professions (...)*".
[53] Article 2 (e) of the Unfair Commercial Practices Directive.
[54] Freely translated from the French version of the BDPA Recommendation on Direct Marketing, *op cit*, p. 8. The BDPA rightfully points out that the term is used, e.g in recital 47 or article 21.2 of GDPR but never receives a proper definition.

Where a direct marketing communication is directed towards a particular individual, the abovementioned lack of protection under consumer law could be mitigated by the rules set out under the GDPR as their sender will be subject to far-reaching information obligations (including the disclosure of the data controller's identity under Article 13 (1) (a) GDPR, the purposes for which their personal data is processed (c), the recipients or the categories of recipients of the personal data (e), the categories of personal data and their further processing purposes under Article 14 (1) (c) and (d)), especially if they intend to rely on consent as a legal base for processing or additionally, be informed of the right to object to processing for direct marketing purposes under Article 21 (1) GDPR if the sender relies on legitimate interests as a ground for processing. For example, the BDPA recently sanctioned a non-for-profit organisation for sending e-mails to subscribers without informing them about their right to reject the processing of their personal data, nor allowing for the effective exercise of such right, outside of any marketing of a product or service.[55]

If this communication includes the placement of cookies on a consumer's remote computer, they will have to be provided with the same clear and comprehensive information based on the GDPR and the sender will necessarily have to rely on the user's prior consent to proceed.[56]

The communication of political opinions, religious or philosophical beliefs may involve the processing of related personal data, which will fall under the definition of "sensitive data" (Article 9 GDPR). These will require explicit consent from the data subject, and give them an additional protection as they will have to actively consent to such processing.[57]

However, for those non-commercial ads that are not directed to individuals using their personal data, the issue remains that the "consumers" will not enjoy protection from either the GDPR or the CEL and this point should equally be further addressed. A first step is to be found in the proposed e-Privacy Regulation which specifies in its recital 32 that advertising does not only cover the offering of product and services for commercial purposes but also "messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties" and "messages sent by other non-profit organisations to support the purposes of the organisation".[58]

3.2 Identifiability of the "Commercial" Communication

Consumers should be able to identify a communication or the media on which it is conveyed as constituting "advertising". Recital 29 of the Directive on electronic commerce already provided that such transparency requirements met the interests of consumer protection and fair trading, taking into account that such communication is essential for the financing of information society services and for developing a wide variety of new, charge-free services.

Recent legislative efforts take into account the fact that consumers rely increasingly on consumer reviews and endorsements when making transactional decisions and introduces requirements to provide that consumer with information on other consumers' reviews, such as their actual use of the product – or that the reviewed constitutes a paid endorsement. Moreover, enterprises are obliged to put the appropriate checks in place to ensure the reality and veracity of such reviews.[59] Specific forms of audio-visual advertising, such as product placement, are regulated as well, if not forbidden when used in programmes targeting children.[60]

---

[55] See Decision n°32/2020 of 16 June 2020 of the BDPA, available at: https://autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-32-2020.pdf. Accessed 18 August 2020. The BDPA doesn't specify the activities in which this NPO was involved. In this case, the sanction from the BDPA was also justified by the complete lack of cooperation from the data controller throughout the BDPA's prior investigation.

[56] Article 129 of the Electronic Communications Act.

[57] However, for existing or former members of a political or religious organisation, or people having regular contact with it, that organisation could rely on the exception set out under article 9 (2) (d) GDPR to process personal data in the course of its "legitimate" activities with appropriate safeguards, and provided that such collected personal data are not disclosed outside the organisation without the data subject's consent.

[58] Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58 (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD). The article 29 Working Party noted however that this consideration was only mentioned in a recital and should be reproduced in proper articles dealing with direct marketing - See Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58), adopted on 4 April 2017. Accessed on 25 May 2020. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

[59] See Recital 47 of the Omnibus Directive; Recital 25 and article 5 of the P2B Regulation.

[60] See recitals 32 and 34 of the AVMS Directive.

This issue is particularly relevant for weaker groups of consumers such as children, senior consumers or disabled people. Studies have shown that children are receptive to ads from digital influencers (eg. through social media, "vlogging" or gaming platforms), creating their own content and with whom children can identify more easily than with "traditional celebrities", resulting in a lack of consciousness that their "interaction" with the influencer consists in receiving commercial communication around a product or service.[61] Moreover, as far as AI will be used, concern has been raised that the same population groups create an emotional bond with a virtual machine, for instance embodying a friendly or reassuring figure, and lack judgment as to the communication and "instructions" that they will receive from it.[62]

However, the lack of a general and technology neutral norm on identifiability dealing with these new forms of advertising could create interpretation issues.

The Belgian regional implementing AVMS decrees[63] contains rules that appear more precise and stricter than those of the CEL, not only in terms of content (exclusion of specific advertising techniques, products[64] or features) but also regarding specific types of communication (sponsorship,[65] product placement[66], on-demand programs,[67] television advertising[68]). For other types of content, self-regulation is also encouraged,[69] such as for accessibility, as well as direct marketing, profiling and behaviourally targeted advertising for minors[70], alcoholic beverages and "junk food"[71] in all audio-visual commercial communications, including now, video-sharing platforms.[72]

These rules will however be limited to media services falling under the scope of the AVMS Directive. Some regret that the EU continues taking an approach that specifies the audio-visual media services to which such rules apply, with a relative lack of clarity as to its exact scope, whereas a more general approach would achieve a better protection of the recipients of such ads. In the area of digital services, EU policy tends to work in silos, distinguishing between all types of services whereas a rather horizontal, layered approach would be necessary with a regulation applying to all types of media indistinctly.[73]

Moreover, even if applied to a media covered by the AVMS Directive, rules on user-generated content (in which will lie posts by vloggers, influencers or influ-gamers for instance) are only applicable to the extent that the communication is made with a commercial intent, and that either the platform or the poster has editorial

[61] V. Verdoodt and N. Feci, Digital Influencers and vlogging advertising: Calling for awareness, guidance and enforcement, A&M, 2018-2019/1, p. 11-22. See, from the same author: V. Verdoodt, Kinderrechten en reclamewijsheid in het digitale tijdperk - Richting een empowerend regelgevend kader voor commerciële communicatie, D.C.C.R., 2019/3, n° 124, p. 3-13.

[62] Pt 3 of European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C252/25), available at:https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017IP0051&from=EN. Accessed on 25 may 2020. On the need to protect children against personalised or behavioural advertising, articles 6 (a) (2) and 28 (b) (3) in fine of the revised AVMS Directive provide that the processing of personal data of minors collected or otherwise generated by media service providers cannot be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. Such collection of children personal data will inevitably happen due to the obligation of the media service providers to put child protection mechanism systems. As personal data will be processed for the sole purposes of the functioning of such systems, these providers should not reuse the children's personal data for commercial purposes (Recital 21 of the AVMS Directive).

[63] See footnote n°36.

[64] Such as the advertising of cigarettes, alcohol or prescription medicines – see article 9 of the AVMS Directive.

[65] Article 10 AVMS Directive.

[66] Article 11 AVMS Directive.

[67] Articles 12 and 13 AVMS Directive.

[68] Articles 19 to 26 of the AVMS Directive and article 27 of the AVMS Directive which specifically deals with protection of minors.

[69] According to the EU Commission, experience has shown that both self- and co-regulatory instruments, implemented in accordance with the different legal traditions of the Member States, can play an important role in delivering a high level of consumer protection. See Recitals 13 and of 14 of the AVMS Directive.

[70] Article 6a AVMS Directive.

[71] Articles 9 (3) and (4) AVMS Directive. Under "junk food", we are referring to the description in the AVMS Directive "foods and beverages containing nutrients and substances with a nutritional or physiological effect, in particular fat, trans-fatty acids, salt or sodium and sugars, of which excessive intakes in the overall diet are not recommended. Member States and the EU Commission can themselves adopt codes of conducts in these areas.

[72] Article 28b of the revised AVMS Directive. Regarding this latter category, the EU Parliament has recently issued guidelines trying to clarify which audio-visual media services were captured under the provisions applicable to video-sharing platform services when the latter constitutes their "essential functionality". See EU Commission Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive (2020/C 223/02), 7 July 2020, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0707(02)&from=EN. Accessed 25 September 2020.

[73] J.-F. Furnémont, Directive SMA : une gouvernance renforcée au service de règles dépassées?, A&M, 2017, n°3, p. 304-311. This author explains that such approach is currently quite difficult due to the rigidity of the decisional processes of EU institutions, since various subjects are dealt with at different directorates within the EU Commission, different ministers at the European council and different commissions within the EU Parliament.

responsibility, which, in the latter case, is less evident considering the number of intervening parties in creating the content.[74]

The same issue can be found in the (self-regulatory) guidelines adopted by the BEJA on influencers[75] and on native advertising,[76] for which an identification obligation only exists if the "influencer" (i) receives a counterpart from the business willing to have its goods or services promoted (either cash or any other advantage) and (ii) on which the business has decisional power over the communication's content.

This means that in cases where a business is paying a user of a social network or audio-visual service to promote a product or a service, without making any decision on how this communication will take place and thus not exercising any editorial control, such promotion would not be subject to the identifiability requirements. Naïve influencers would bear full editorial responsibility for commercial communications of products or services, although they do not specifically act as professionals and may not be even aware that their post constitutes an ad, nor have the purpose of realising a commercial communication.[77]

These issues could be mitigated by the fact that the general norm for unfair commercial practices contained under the CEL is broad enough to cover any breach of legislation could constitute an unfair commercial practice, be it local laws beyond the rules of the CEL, international laws of self-regulatory codes of conduct. The issue with the latter category lies with the fact that the business should be a signatory of that code for there to be a breach and subsequent unfair trade practice. [78]

The "Black list" of commercial practices under the CEL includes the use of editorial content in the media – paid for by a business - to promote a product or service without making this clear in the content or by images or sounds easily identifiable by the consumer,[79] as well as the inclusion in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them,[80] and unauthorised online direct marketing.[81]

Finally, the rules on unfair competition could be useful to denounce practices that are, in appearance, legitimate but remain unfair when considering their specific target audience, mostly when children are involved, even though, in the latter case, some scholars plead for the adoption of a specific set of rules protecting this sensitive audience.[82]

For the identifiability requirement, the Omnibus Directive provide for additional rules that could address these concerns, without considering the type of media concerned nor the existing editorial liability of neither the business nor the intermediary.

On the one hand, (i) the fact that a business provides search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of product within the search results, (ii) stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers and (iii) submitting or commissioning another legal or natural person to submit false consumer reviews

[74] See on this topic V. Verdoodt and N. Feci, Digital Influencers and volgging advertising: Calling for awareness, guidance and enforcement, A&M, 2018-2019/1..

[75] Recommandations du Conseil de la Publicité en matière d'influenceurs en ligne (in Dutch: *Aanbevelingen inzake online influencers*), October 2018 (date not further specified), available at: https://www.jep.be/sites/default/files/rule_reccommendation/code_en_matiere_didenti fication_des_publicites_natives_et_communications_commerciales_connexes.pdf. Accessed 13 April 2020).

[76] Code en matière d'identification des publicités natives et communications commerciales connexes (in Dutch: *Code over herkenbaargeid van native advertising en aanverwante commerciële communicatie*), 12 December 2018 (published 4 January 2019), available at: https://www.jep.be/sites/default/files/rule_reccommendation/code_en_matiere_didentification_des_publicites_natives_et_communications_commerciales_connexes.pdf. Accessed 12 April 2020.

[77] See also V. Verdoodt, Aanbevelingen voor online influencer-marketing van de Raad voor Reclame, D.C.C.R., 2018/3-4, n°120-121, p. 241-243.

[78] G. Sorreaux, Publicité et étiquetage des denrées alimentaires, Bruxelles, Editions Larcier, 2016, p. 49-50.

[79] Article VI.100, 11° CEL.

[80] Article VI.103, 5° CEL.

[81] Article VI.103, 3° CEL. Under this bullet, the CEL is referring to unauthorised direct marketing as marketing not authorised by law, be it under article VI.110 (unsolicited communications), XII.13 (direct marketing by e-mail), or a specific law or regulation authorising direct marketing in order to perform a contractual obligation.

[82] See H. Jacquemin, Chapitre 8 - Protection du Consommateur et numérique en droits européen et belge, in: Vulnérabilités et droits dans l'environnement numérique, Bruxelles, Editions Larcier, 2018, p. 244. See also, on this specific question, V. Verdoodt, Kinderrechten en reclamewijsheid in het digitale tijdperk - Richting een empowerend regelgevend kader voor commerciële communicatie, D.C.C.R., 2019/3, n° 124, p. 3-13.

or endorsements, or misrepresenting consumer reviews or social endorsement, in order to promote products, are all added into the "black list" of commercial unfair practices.[83]

On the other hand, when a business gives access to consumer reviews of products, it should provide information about whether and how the business ensures that the published reviews originate from consumers who have actually used or purchased the product. Failure to do so will be deemed an omission of information qualifying as a misleading commercial practice.[84] A similar obligation is inserted for the business exploiting an online marketplace to specify whether the third party offering the product is a trader or not based on the declaration that third party made to that business.[85]

4. Personalisation : Providing the Consumer with a Tailor-made Communication or Product, with or without Automated Means

The increasing use of automated means, such as AI, to create personalised commercial communications, services and products shows a shift of the market towards a consumer-centric (or human-centric) approach, defined by the EU Commission as "an international approach that promotes the respect of fundamental rights, including human dignity, pluralism, inclusion, non-discrimination and protection of privacy and personal data".[86]

"Personalisation" in itself, with or without automated means should be considered a commercial practice which can potentially have an influence on the consumer's behaviour and their decision over a transaction.[87]

The legal literature accepts that the performance of an agreement using AI and involving personal data could lead to an automated processing of personal data under Article 22 GDPR if there was no human intervention at all in it. In its Proposal for a Regulation on the liability for the operation of AI-systems, the EU Parliament confirms that AI is a form of "automated decision-making", defined as a "situation in which a user initially delegates a decision, partly or completely, to an entity, by means of software or a service. That entity, in turn, uses automatically executed decision-making models to perform an action on behalf of a user, or to inform the user's decision in performing an action".[88]

Both elements combined challenge again some of the existing rules on consumer and unfair competition laws (including consumer information) and on data protection (including the rules applicable to automated processing of personal data, and the principles of accountability and privacy by design under the GDPR), and show that a convergence of both sets of legislation is necessary to guarantee consumers empowerment (or "agentivity")[89] in the exercise of their rights, allowing them to maintain control over their decision-making process and the communication of their personal data. This, in turn, ensures that the enterprise can achieve a proper personalisation of the consumer needs and process relevant quality data to achieve these purposes using automated means.

[83] See article 3 (7) (a) and (b) of the Omnibus Directive adding, respectively, pts 11a, 23b and 23c to Annex I of the Unfair Commercial Practices Directive.
[84] Article 3 (4) (c) of the Omnibus Directive.
[85] Article 3 (4) (a) (ii) of the Omnibus Directive. On this latter obligation, one can wonder why the provider of online platform service does not have an active duty to verify the identity of such third party, as is the case for consumer reviews, or an obligation to put the appropriate checks in place.
[86] See European Commission White Paper on Artificial Intelligence - A European approach to excellence and trust, 19 February 2020. Accessed on 10 May 2020. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, p. 9. Under p. 13, the EU Commission considers that legislation could be improved especially regarding product safety, liability and transparency.
[87] F. Jacques, Personnalisation des prix - Regard européen sur la pratique, R.D.T.I., n°78-79, 2020, p. 59; H. Jacquemin, Le big data à l'épreuve des pratiques du marché et de la protection du consommateur, R.D.T.I, 2018/1, n°70, p.75-91.
[88] European Parliament report of 5 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), available at: https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.html, p. 16. Accessed 28 November 2020. The idea that a human facing the use of AI for a commercial transaction, whether or not involving the processing of its personal data, was already debated before. See Independent high-level Expert Group on Artificial Intelligence set up by the European Commission, Ethic Guidelines for Trustworthy AI, 8 April 2019, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 . Accessed 10 May 2020. p. 18.
[89] C. Zolynski, Protection + Agentivité, la nouvelle équation pour penser les relations entre consommateurs et intelligences artificielles, Ent. & L., 2019, n°6, pp. 331-341.

4.1 Consumer Information

4.1.1 Consumer Laws

In terms of consumer contracts, an enterprise is under the obligation to inform the consumer on the total price of the goods or services, or, if such price cannot be calculated in advance, the manner in which the price is to be calculated as well as all additional charges and whether those are included in the price or not.[90] This information obligation could even be more general, to the extent that the sold good or service is personalised, with or without the use of automated means, taking into account the obligation for an enterprise to inform the consumer in relation to the main characteristics of the goods and services.[91]

This set of rules reinforces the rules of civil law on consent requiring that the contractual counterparty, taking into account a possible imbalance of power[92] (because he or she is a consumer) is provided with the necessary information allowing it to engage "wilfully and knowingly".

If an enterprise fails to provide information to the consumers in a clear and understandable manner (either because it is missing, false, or presented in a way that it is confusing to the consumer), this will be considered a misleading commercial practice. More specifically, it seems that the business would be under a broad obligation to explain the rationale and methods used behind the personalisation of a good or service since not providing information in relation to its "(…) benefits, risks, execution, composition, (…) method and date of manufacture or provision (…), specification"[93] would constitute a misleading commercial practice.

Regarding the price, the lack of information or misleading information in relation to a price, or the manner in which it is calculated, or the existence of a specific price advantage is also already considered a misleading commercial practice.[94]

The idea has been debated in legal literature that an enterprise's information obligation towards the consumer should cover the use of AI, and include the disclosure that the entity with whom the consumer interacts prior to a transaction is not a human.[95] Such is the case when the consumer is interacting with virtual assistants or *chatbots*, while having the impression that he or she communicates with a human of flesh and blood who is there to – and wants to – help the consumer complete that transaction. It was suggested that this information should also contain a disclosure of the logic behind the algorithms used underlying this interaction.

Where Belgian law in its current state does not provide for such specific obligations, the Omnibus Directive provides two new requirements that will need to be implemented under the CEL.

First, Article 6 of the Unfair Terms Directive, implemented under Article VI.45 CEL, is updated to include, as information to be provided prior to the conclusion of a "distance contract", the fact that the price was personalised based on automated decision-making.[96] When it does apply, this rule allows the consumers to consider the potential risks in their purchasing decision. However, this requirement is met with two issues. First, the level of information detail that must be provided to the consumer, while ensuring that such information is provided to them in a clear and understandable manner, or the extent to which the enterprise should explain the functioning of the algorithms funding the automated decision, remains unclear and should be subject to further guidance.

This new requirement also does not apply if personalisation was achieved through means other than automated processing, such as "real-time" or "dynamic" pricing. These techniques involve changing the price in a highly flexible and quick manner in response to market demands when those techniques do not involve personalisation based on automated decision-making.[97] Therefore, an enterprise that does not recourse to a personalised automated decision-making but still adapt their prices using other real-time technologies such as cookies, tracers or other

[90] Article VI.2, 3° CEL (general information obligation) and Article VI.45,3° CEL for distance contracts.
[91] Article VI.2, 1° CEL (general information obligation) and Article VI.45,1° for distance contracts.
[92] This seems to be systematically the case for a consumer navigating in an online environment, who does not have any leverage to negotiate or waive some of the terms of a business prior to entering the transaction.
[93] Article VI.97,2° CEL (misleading information) and VI.99, §4, 1° CEL (omission of information).
[94] Article VI.97, 4° CEL. (misleading information) and VI.99, §4, 3° CEL (omission of information).
[95] J.-B. Hubin and H. Jacquemin, Titre 3 - L'intelligence artificielle: vraie ou fausse amie du justiciable? - Enjeux du recours à l'IA par les avocats, assureurs et legaltechs, In: Le juge et l'algorithme: juges augmentés ou justice diminuée?, Editions Larcier 2019, p. 75-104.
[96] Article 4 (4) (a) (ii) of the Omnibus Directive, inserting a pt (ea) under article 6 (1) of the Unfair Terms Directive.
[97] Recital 45 of the Omnibus Directive.

indicators can continue practicing different prices, and potential discrimination between consumers would not be covered by this obligation.

Second, Article 7 of the Unfair Commercial Practices Directive, dealing with misleading omissions, provides for a list of material information to be provided to the consumer, and is implemented under Article VI.99, §4 CEL. This list is updated by the Omnibus Directive[98] to include a disclosure of the main parameters determining the ranking of products presented as a result of the consumer's search query when browsing the enterprise's website, and the relative importance of those parameters. "Ranking" is defined as the relative prominence given to products, as presented, organised or communicated by the enterprise, irrespective of the technological means used for such presentation, organisation or communication.[99] This addition may be of limited use regarding AI as the Omnibus Directive sets that such disclosure is without prejudice to the protection that enterprises may enjoy under the Trade Secrets Directive.[100] If the AI and the algorithms designed for its functioning are protected by trade secrets, the amount of information that an enterprise would have to provide without breaching any law would be limited. Moreover, the Omnibus Directive adds that enterprises should not be required to disclose the detailed functioning of their ranking mechanisms, including algorithms, but could rather limit it to a general description of the main parameters determining the ranking, and their relative importance as opposed to other parameters.[101]

Aside from new legislation, F. Jacques[102] considers that an enterprise can also undertake misleading commercial practices even if the information that it provides to the consumer is factually correct regarding the price or its means of calculation. For example, applied to personal rebates, a business could present a price as discounted specifically for the consumer whereas such price has been reduced beforehand based on personalisation using the consumer's shopping behaviour data. In doing so, the information provided on the price would be prima facie correct, but presented in such a way that the consumer is misled as to its means of calculation.

He also pleads that the concept of personalisation as a whole should be disclosed to the consumer and that not doing so would constitute an unfair commercial practice: consumers have shown that information regarding personalisation (the price and its means of calculation) could be considered as "material", the EU Commission further explained in its guidance document on the implementation of the Unfair Commercial Practices Directive that compliance with the rules on the protection of personal data needed to be considered when conducting the assessment, profiling or personalisation in breach of these rules amounting to an unfair commercial practice,[103] and the same guidance document treats the lack of consumer information regarding personal data processing going beyond the transaction with the enterprise, e.g for marketing purposes, as the omission of a material information.[104] The lack of information on personalisation therefore undoubtedly results in the consumer making a commercial decision that he or she would not have taken had he or she been informed thereof.

4.1.2 Under Data Protection Laws[105]

When using automated means, a fair and transparent processing of personal data under the GDPR requires the data controller to provide meaningful information about the logic involved in the decision made (Articles 13 (2)(f) and 14 (2) (g)).

Such explanation should not necessarily be a complex overview of the algorithms used or a disclosure of the full algorithm. The information provided should however be sufficiently comprehensive for the data subject to

[98] Article 3 (4) (b) of the Omnibus Directive, inserting a paragraph 4a under article 7 of the Unfair Commercial Practices Directive.
[99] Article 3 (4) (b) of the Omnibus Directive, inserting a point (m) under article 2 of the Unfair Commercial Practices Directive.
[100] Directive 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, OJ, 2016, L 157, p. 1.
[101] Recital 23 of the Omnibus Directive.
[102] F. Jacques, Personnalisation des prix - Regard européen sur la pratique, R.D.T.I., n°78-79, 2020, p. 60-62.
[103] European Commission Staff Working Document of 25 May 2016. Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices 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 – A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses; COM (2016) 320 final, SWD, 2016, 163 final, p. 24. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016SC0163. Consulted on 18 August 2020.
[104] *Ibid.*, p. 63; N. Van Eijk, C. J. Van Hoofnagle and E. Kannekens, Unfair Commercial Practices: A Complementary Approach to Privacy Protection, E.D.P.L., n°3, 2017, p. 334: these authors see a strong overlap between the omission of material information under article 7 of the Unfair Commercial Practices Directive and the information obligation from the data controller when collecting personal data under articles 13 and 14 GDPR.
[105] See also R. Steppe, Prijsdiscriminatie in het digitale tijdperk. Beschouwingen over de nieuwe Algemene Verordening Gegevensbescherming i), n R. Steppe, M. Storme, F. Helsen (eds.), Innovatie en disruptie in het economisch recht, 2017, pp. 105-149.

understand the reasons for the decision made concerning him or her. The Article 29 Working Party adds that complexity is no excuse for failing to provide information to the data subject, which is particularly relevant in a technologically complex environment involving many actors.[106] This is undoubtedly the case when AI comes into play, and that the business, the operator, the engineer, and the software designer of the same AI system used in the framework of a single consumer transaction are different people.

Unlike the rules brought by the Omnibus Directive, this appears to be a general requirement that is not limited to specific categories of information such as price or ranking, and could reinforce a possible lack of information regarding the general rationale behind the algorithms used under consumer laws.

4.2 Privacy by Design and Accountability Principle

When using personalisation techniques, with or without automated means, the enterprise faces specific questions under privacy laws, based on the accountability principle (Article 5 (2) GDPR). For instance, it must ensure that its processing activities comply with its GDPR obligations both at the time of determining the means for processing and during the processing itself, it must implement appropriate technical and organisational measures, designed to implement the data-protection principles, such as data minimisation, in an effective manner and must integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects.[107]

4.2.1 Finding the Appropriate Legal Basis for Processing of Personal Data

An important question to consider for the controller is which legitimate ground to use to process personal data, the main legitimate grounds being consent (Article 6 (1) (a) GDPR) and legitimate interest (Article 6 (1) (f) GDPR).[108]

To rely on consent, the data controller will need to ensure that the data subject's consent is (1°) freely given, (2°) specific, (3°) informed and (4°) unambiguous.

The processing for legitimate interests of the controller would be subject to the conditions that (1°) the interests of controller must be legitimate,[109] (2°) the processing of personal data must be necessary for the realisation of controller's objectives and (3°) a necessary balance must take place between the interests, freedoms and fundamental rights of the data subject and the data controller's own interest.

Consent, under the strict conditions of the GDPR, has long been seen as the most appropriate way to ensure that the data subject is correctly informed and accepts the processing of its personal data with knowledge of things, and enjoys a comparable level of pre-contractual information as the one under consumer laws.

However, obtaining valid consent following the GDPR appears burdensome or no longer adapted to the current state of advertising technologies.

On the other hand, legitimate interest is seen as increasing an asymmetry of information between consumers, data subjects, and enterprises, data controllers and cannot be used as legal basis in some circumstances. It is therefore uncertain that it can provide an effective alternative to consent for personalisation.

---

[106] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017 and last revised on 6 February 2018. Accessed on 15 May 2020. Available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826, p. 25.

[107] Articles 24 and 25 GDPR.

[108] The performance of a contract (Article 6 (1) (b) GDPR) is another possible processing grounds but is not considered in detail in this contribution. We briefly touch upon it when discussing consent and the New Deal for Consumers below.

[109] Recital 47 GDPR states that direct marketing can be, in itself, a legitimate interest of the data controller. The WP29 specified that the interest is legitimate, as long as it is in compliance with data protection and other laws. Belgian scholars have deemed this approach too restrictive and the interests should also be assessed under the lights of fairness and transparency, which are required for any personal data. Moreover, these interests would necessarily include compliance with fundamental rights. Therefore, personalisation based on legitimate interests should take place in compliance with such fundamental rights and a data controller should avoid any breach of, inter alia, the anti-discrimination laws mentioned above. See Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directive 95/46, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 9 May 2020; J.-F. Puyraimond, L'intérêt légitime du responsable du traitement dans le RGPD: in cauda venenum?, D.C.C.R., 2019/1-2, n°122-123, p. 52. See also D. Goens, Data protection bij financiële instellingen, 2018, Anvers - Cambridge, Intersentia, p. 246.

Several issues arise, calling both the effectivity of both grounds into question, and a reflection from the enterprise is needed to anticipate these issues.

4.2.1.1 Privacy Fatigue

"Informed" consent requires that the data controller provides sufficiently transparent information beforehand, in a clear and intelligible language, on the processing of personal data, at the time personal data is directly collected by the data controller (Article 13 GDPR) or within a reasonable term when that data is indirectly obtained (Article 14 GDPR).

Providing information to data subjects prior to obtaining their consent is essential to enable them to make informed decisions and exercise their rights. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.[110] On this aspect, the GDPR expressly refers to the requirements set out under the Unfair Terms Directive: information must be concise, easily accessible and in an easy to understand and plain language and, additionally, where appropriate, visualisation be used.[111] This is welcomed in situations where there are a lot of actors involved and the technological complexity of a practice makes it difficult for the data subject to know and understand whether, by whom and for what purpose, personal data relating to him or her are being collected, such as in the case of online advertising.[112] Moreover, the data subject should be able to consent by means of written declaration (express or functionally similar, such as ticking a box), after being given the possibility to read the information, contained in terms and conditions, regarding the processing.[113]

Recently, the ECJ clarified that the same information obligation also applied for cookies, and that the controller needs to inform the data subject on the duration of such cookies and the possibility for third parties to have access to them, in order to guarantee transparent information.[114]

In the meantime, the BDPA applied similar principles and fined a website specialised in legal news, which cookies policy was neither compliant with GDPR, nor with Article 129 of the Act on Electronic Communications.[115]

The requirement that consent must be specific reinforces this information obligation. The data subject needs to be able to distinguish between different purposes for the processing of their personal data and choose to which ones they want to agree (the "granularity of consent").[116] In terms of cookies for instance, two different consents would be needed for analytic cookies and for functional cookies.[117] This requirement also prevents the data controller to rely on consent for other purposes than those for which it was originally obtained. In terms of personalisation, a data controller would need to obtain a separate, second consent from the consumer to create specific profiles if it first obtained their personal data for direct marketing communication purposes.

This results in consumers being confronted with a substantial amount of information and steps to be taken when surfing the Internet, on each merchant website they visit, which is necessary to obtain their consent for the enterprise's processing purposes. The BDPA,[118] the EDPB[119] and Belgian scholars share the view that this could

---

[110] Guidelines 05/2020 of 4 May 2020 of the EDPS, on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Accessed 10 May 2020, n° 62, p. 14.

[111] Recital 42 GDPR. Recital 38 and 58 GDPR specify that such information should be adapted to its target audience. Where children are targeted, such information should be in a clear and plain language that the child can easily understand, especially when direct marketing or the creation of personality or user profiles, is used to provide them services.

[112] Recital 58 GDPR.

[113] Getting the consumer to accept terms and conditions that they did not have the possibility to acknowledge would constitute an abusive contractual clause and, in turn, an unfair commercial practice under article VI. 83, 26° CEL.

[114] CJEU, 1 October 2019, case C-673/17, *Planet49*, ECLI:EU:C:2019:801.

[115] Decision n° 12/2019 of 17 December 2019 of the BDPA, available at: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-12-2019.pdf. Among other breaches, the website provided incomplete information to its users regarding cookies (article 12 GDPR), used pre-ticked boxes to obtain users' consent to the use of cookies, and the data controller used legitimate interest as a processing ground for analysis cookies. On this last point, the BDPA points out that the current rule provides that only strictly necessary cookies are exempt from prior consent from the data subject but does not exclude that the rule could be extended to other types of cookies in the future, in the framework of the reform of the e-Privacy Directive.

[116] EDPB Guidelines 05/2020 of 4 May 2020 of the EDPS, on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Accessed 10 May 2020, n°56, p. 13.

[117] BDPA Recommendation on Direct Marketing, p. 63.

[118] *Ibid.*, p. 67.

[119] Referring to "Click-fatigue", EDPB Guidelines 05/2020 of 4 May 2020 on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, consulted on 10 May 2020., n°87-89, p. 18.

lead to a loss of control over the personal data communicated by the consumers, as they will tend to be less vigilant, and experience a real "privacy fatigue", where they will mechanically consent or refuse processing.

A more effective and reasoned approach to consent however is possible but would rest on the enterprise's willingness to communicate that prior information to the consumer in an effective and friendly manner: the works of R. Ducato[120] have shown that "informed consent" is not the issue as such, but rather the means that the controller uses to convey information to the consumer. Privacy fatigue could be avoided by giving consumers a sense of control and agentivity over their personal data if techniques other than the provision of lengthy privacy policies are used: relying on new technology (videos, multi-layered menus, chatbots or other types of electronic assistants), techniques that require a more active interplay with the consumer (questionnaires or "privacy" mini-game).[121] The BDPA and EPDB also suggest alternative techniques where the data subject makes a specific movement with the mouse or finger on the controller's webpage, or repeats a phrase orally using a microphone. However, in the new version of its guidelines on consent, the EDPS specified that based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity would not be sufficient, since such actions are difficult to distinguish from other activity or interaction by a user.[122]

On the other hand, relying on legitimate interest for processing personal data would also require that data subject is informed under Articles 13 and 14 GDPR.

4.2.1.2 Freedom to Consent and Agreements under the New Deal for Consumers

The data subject must be able to *freely accept* or refuse the processing of its personal data, without being deprived of the intended service or performance from the data controller. The GDPR forbids that a service be subject to a consumer's prior consent to have their personal data processed for purposes that are not necessary for the performance of an agreement (Article 7 (4) GDPR). Equally, the data subject should be able to withdraw consent without enduring negative consequences (such as exaggerated costs for withdrawal).[123] On the other hand, it seems possible for the data controller to continue providing specific advantages to those data subjects who did not withdraw their consent, or that the latter can continue benefitting from additional services.[124]

Free consent also entails that the data subject should also be able to consent outside of any inappropriate pressure or influence. For example, the BDPA recently sanctioned a business which required its customers to share their electronic identity card and have its content read in the shops to create a fidelity card, without providing a valid alternative to do so. Consequently, consumers could not validly consent to the processing of their personal data to obtain a fidelity card since if they refused to do so, they would not obtain the same advantages and promotions as the customers enjoying it.[125]

---

[120] See R. Ducato and A. Strowel, Information duties between consumer and data protection in the "Internet of Platforms": promoting awareness by design, D.C.C.R., 2019, n°122-123, p. 123-149; A. Rossi, R. Ducato, H. Haapion and S. Passera, When Design Met Law: Design Patterns for Information Technology, D.C.C.R., 2019/1-2, n°122-123, p. 79-12.

[121] See also, sharing the same opinion: F. Jacques, Personnalisation des prix - Regard européen sur la pratique, R.D.T.I., n°78-79, 2020; H. Jacquemin, Le big data à l'épreuve des pratiques du marché et de la protection du consommateur, R.D.T.I, 2018/1, n°70, p.75-91.

[122] It would also not be possible to allow the data subject to withdraw his or her consent as easy as he or she has given it, see Guidelines 05/2020 of 4 May 2020 of the EDPS, on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, consulted on 10 May 2020, n° 86, p. 18.

[123] Guidelines 05/2020 of 4 May 2020 of the EDPB on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, consulted on 10 May 2020, n°13., p. 6. The guidelines consist in a "slightly updated version" of the Article 29 Working Party Guidelines of 10 April 2018 on Consent under Regulation 2016/679 (WP259.01), which were endorsed by the EDPB.

[124] Y. Poullet, Consentement et RGPD: des zones d'ombre !, DCCR, 2019/1-2, n°122-123, p. 6.

[125] Decision n°06/2019 of 17 September 2019 of the BDPA, available (in Dutch) at: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-06-2019.pdf (consulted on 15 March 2020). This decision was later annulled by the Belgian Market Courts, as *inter alia*, the BDPA had based its reasoning on legislation on electronic-ID which was not yet in force at the time of the breaching behaviour from the data controller, see Markets Court of Brussels, 19 February 2020, n°2019/AR/1600, available in Dutch at: https://www.autoriteprotectiondonnees.be/publications/arret-du-19-fevrier-2020-de-la-cour-des-marches-disponible-en-neerlandais.pdf.

The EDPS recently reviewed its guidelines on consent, complementing the ECJ's *Planet49* case,[126] to condemn the practice of "cookie walls" to obtain consent. Such situations occur where a data controller is subjecting access to its services and functionalities to the user agreeing to the use of cookies.[127]

The upcoming New Deal for Consumers[128] introduces the notion of a consumer agreement the counterparty of which is not money. This cover the cases where the enterprise undertakes to deliver goods or services to the consumer "and the consumer provides or undertakes to provide personal data" to such business, except when such personal data is processed exclusively for the performance of that agreement.[129] The latter processing is subject to a different legal basis under Article 6 (1) (b) GDPR.

When the first versions of the text had been adopted, the EDPB had raised the concern that the grounds for processing under Article 6(1)(b) GDPR would be unduly relied upon, as a data controller would consider that personal data is simply the "counterpart" for receiving the goods or services, just as any payment in money, and rely on the consent to enter into an agreement rather than informed consent under Article 6 (1) (a) GDPR.[130] Also, this new kind of agreement would entice data controllers to take recourse to "tied in" or "bundled" consent, by which the performance of the agreement only occurs if personal data has been provided by the consumer.[131]

The exception in its current state seems to inform enterprises that they cannot use personal data originally collected for the strict performance of an agreement, for further (marketing) purposes. However, it is doubtful that it will effectively remedy the issue related to tied-in consent. Article 6 (1) (b) GDPR is limited in scope as it only covers processing that is "strictly" necessary for the performance of an agreement and therefore cannot be relied on if a data controller can reach the same purposes through other means.[132] In the cases where an enterprise cannot or does not need to rely on Article 6 (1) (b) GDPR to actually perform its agreement with a consumer, it can still be collecting personal data using consent, and be tempted to make it conditional on the provision of goods or services. In this understanding, the need for the consumer to provide consent and its reach can still be source of confusion if the consumer is not provided with proper information, since they still could be led to believe, wrongly, that the provision of their personal data is necessary to carry on a transaction with the enterprise.

In order to avoid such confusions, a data controller could be tempted to rely on legitimate interest instead of consent. However, in the current state of the law, the issue linked to cookies remains since their placement on a data subject/consumer's device still require their consent, whether or not personal data is processed.[133] The same issue arises for direct marketing communications sent by e-mail.[134] Moreover, "explicit" consent will also be mandatory when the data controller seeks to process sensitive personal data under Article 9 GDPR such as race or ethnic origin, political opinions, religious or philosophical beliefs, as well as health data. The processing of sensitive personal data is forbidden unless the data controller can rely on one of the exceptions set out under Article 9 (2) GDPR, among which explicit consent, and this seems to be the only relevant exception in the

[126] CJEU, 1 October 2019, case C-673/17, *Planet49*, ECLI:EU:C:2019:801. This case-law did not envisage cookie walls as such but deals with the question of "unambiguous" consent, as defined under the GDPR, in relation with the placement of cookies and tracking on a user's device using pre-ticked consent boxes.

[127] Guidelines 05/2020 of 4 May 2020 of the EDPS, on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, consulted on 10 May 2020, n°39, p. 11.

[128] Namely, the Omnibus Directive, but also the Digital Contents Directive (Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ, 2019, L 136, p. 1.) and the new Sales of Goods Directive (Directive 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ, L 136, 2019, p. 28). The last directive is not envisaged in this contribution.

[129] Recital 31 Omnibus Directive, and article 4 (2) inserting an article 3 (1a) in the Consumer Rights Directive.

[130] Opinion 8/2018 of the EDPS, on the legislative package "a New Deal for Consumers", available at: https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf, pp. 14-16.

[131] *Ibid.*, p. 17; Recital 43 and article 7 (4) GDPR.

[132] Guidelines 2/2019 of 8 October 2019 of the EDPS on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf., n°25, p. 8. Accessed on 22 August 2020. According to the BDPA, a possible case where a data controller could rely on such ground is where the data subject and the data controller have entered into an agreement for the sole purpose of receiving direct marketing communication, where personal data would then be processed solely for direct marketing purposes, i.e. the performance of the agreement. See BDPA Recommendation on Direct Marketing, p. 47.

[133] Article 129 of the Electronic Communications Act.

[134] The BDPA mentions as an example unsolicited communication by electronic means, which require prior informed consent from the data subject, and the "soft opt-in" exception related to such communications (see article XII.13 CEL and its executing decree of 4 April 2003, and articles 13(1) and 13(2) of the e-Privacy Directive.

framework of personalisation for promotional purposes, which are not covered by the other available exceptions available under that Article.

4.2.1.3 Imbalance of Power Between the Data Subject and the Data Controller

The use of legitimate interests as a ground for processing remains doubtful as some authors raised concerns that it increases the information asymmetry between the controller and the data subject and, allegedly, does not offer the same protection as consent.

Consent, despite all the information provided, does not seem to eliminate such risk, just as is the case under consumer laws, since big business players enjoying a monopoly and *de facto* stronger power:[135] in most instances, not only will the text of the privacy policy (or the commercial terms and conditions) not be negotiable, but the consumer /data subject will feel compelled to consent either way without having control or leverage as to the information given. This puts into doubt the fact that the consumer has effectively "consented" to the business' commercial conditions and privacy policy.

If the legal grounds of contract and consent do not solve this issue, the obligation for the data controller to provide specific safeguards when relying on legitimate interest could be seen as a sufficient trade-off allowing it to carry on with processing, without the "burden" of consent – which is not an efficient protection for the consumer anyway. The consumer, instead, in terms of safeguards is granted with an absolute right to oppose the processing of personal data for direct marketing purposes[136] and to oppose automated processing, or at least require a human intervention or review of the processing mechanics.[137] Moreover, an additional safeguard is found in the data minimisation and purpose limitation principles, under which a data controller will be prevented from reusing personal data obtained through another legal basis, and will have to assess whether another purpose for processing is compatible with the purpose for which data was originally collected.[138] As a matter of example, the BDPA issued several decisions sanctioning the processing of personal data for electoral purposes, whereas they had originally been collected for another purpose which was deemed incompatible, where one of the data controllers could even potentially obtain financial benefits which is an aggravating factor under Article 83 (2) (k) GDPR.[139]

If data controller correctly complies, in terms of legal design, with providing the consumer/data subject with such remedies (more detailed under section 4.3), this would appear to achieve a fairer balance of powers, combined with a proper information of its rights as consumer/data subject, in a manner that he or she can easily understand.

4.2.2 Influence of Other Legislations

Which the enterprise should consider other applicable laws when designing a(n) automated personalisation solution, especially with regards to pricing.

First, price personalisation is of interest to the EU competition law. Several businesses, using algorithms to categorize individuals to determine prices could, by doing so, proceed to collusion prohibited under Article 101 TFEU or abuse their dominant position. This is particularly the case of major players (such as the GAFAs) pooling their data and enriching each other AI devices, by creating unfairly discriminative prices under Article 102 TFEU. However, such concerns should not be exaggerated as there are doubts as to the actual capacities in the current state of technology of AI to enter into collusive strategies without human intervention. Moreover, there is doubt as to whether such practices would be reprehensible under EU competition law at all, because it is unlikely to happen, or even be beneficial to consumers. The specialists on this topic explain that a business enjoying a

[135] Y. Poullet, Consentement et RGPD: des zones d'ombre !, DCCR, 2019/1-2, n°122-123, p. 6.
[136] Article 21 (2) GDPR.
[137] Article 22 (3) GDPR.
[138] Article 6 (4) GDPR. See also Guidelines 2/2019 of 8 October 2019 of the EDPS on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf. Accessed 22 August 2020, pp. 14-15: the EDPB considers rightfully that profiling or behavioural advertising is not necessary for the performance of an agreement, and their collection, or further use cannot be justified by that fact that behavioural advertising funds the provision of the service.
[139] See Decision n° 04/2019 of 28 May 2019 of the BDPA, available at: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-04-2019.pdf; Decision n°10/2019 of 25 November 2019 of the BDPA, available at: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-10-2019.pdf; Decision n°11/2019 of 25 November 2019 of the BDPA, available at: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-11-2019.pdf). All accessed 18 May 2020.

dominant position would be in a better position to set prohibitive prices without personalisation than with personalisation, since following personalisation everyone would be exactly paying the price that is adapted to them. However, EU competition law remains an interesting tool to deal with the issue of price discrimination as it is flexible and evolves depending on the specific situation at stake and, allow the legislator to determine objectively which behaviours can be deemed anticompetitive in an economy based on algorithms.[140]

Then, as automated personalisation could result in discrimination, businesses will have to contend with an already far-reaching legislation. The Geoblocking Regulation[141] aims, in transnational situations, at preventing geo-blocking and other forms of discrimination based, directly or indirectly,[142] on the customers' nationality, place of residence or place of establishment, or when clients are granted different conditions of access to goods or services, unless objectively justified (Article 4).[143]

Enterprises remain however allowed to design country-specific websites, and choose specific products destined for a target audience, using e.g personalised or dynamic pricing, provided that they treat the customers across the EU in a non-discriminatory manner.[144] Such will be the case for reasons "unrelated to nationality, place of residence or place of establishment",[145] or if the difference of treatment is provided under specific EU or law of a Member State compliant with EU law.[146]

The scope of the Geoblocking Regulation appears however to be limited as it does not apply to all services mentioned under Article 2 (2) of the Services Directive.[147] For instance, the regulation does not apply to non-economic services of general interest, financial services, electronic communications services and networks, transports, audio-visual services or gambling.

At national level, the Belgian Discrimination Act forbids forms of discrimination, in the public and private sector, among others in relation to the access to goods and services put at the public's disposal or the access, participation, and the exercise of any economic, social, cultural or political accessible to the public, which is based on age, sexual orientation, civil state, birth, fortune, religious of philosophical belief, handicap, physical or genetic features and social origin, unless justified for legitimate purposes and where appropriate and necessary means for their realisation have been put in place.[148]

[140] See, on this particular topic N. Petit, Algorithmes tarifaires et droit européen de la concurrence in l'Europe au présent!, Bruxelles, Bruylant,2018, p.167-176 and A. Ittoo and N. Petit, Titre 4 - Algorithmic Pricing Agents and Tacit Collusion: A Technological Perspective, in L'intelligence artificielle et le droit, Bruxelles, Editions Larcier, 2017, p. 241.

[141] Regulation 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 No 2006/2004 and 2017/2394 and Directive 2009/22, OJ, 2018, L 60l, p. 1., article 1.

[142] Recital 6 Geo-Blocking Regulation: "Thus, it also seeks to cover unjustified differences of treatment on the basis of other distinguishing criteria which lead to the same result as the application of criteria directly based on customers' nationality or place of residence, regardless of whether the customer concerned is present, permanently or on a temporary basis, in another Member State, or place of establishment. Such other criteria can be applied, in particular, on the basis of information indicating the physical location of customers, such as the IP address used when accessing an online interface, the address submitted for the delivery of the goods, the choice of language made or the Member State where the customer's payment instrument has been issued".

[143] The Geo-Blocking Regulation distinguishes three types of access to goods or services: (a) the purchase of goods from a trader, where either those goods are delivered to a location in a Member State to which the trader offers delivery in the general conditions of access, or those goods are collected at a location agreed upon between the trader and the customer in a Member State in which the trader offers such an option in the general conditions of access; (b) the customer receives services supplied electronically by the trader, other than services the main feature of which the provision of access to and use of copyright protected works or other protected subject matter, including the selling of copyright protected works or protected subject matter in an intangible form; (c) receives service from a trader, other than electronically supplied services, in a physical location within the territory of a Member State where the trader operates.

[144] Article 4 (2) of the Geo-Blocking Regulation.

[145] Recital 27 of the Geo-Blocking Regulation, listing e.g membership of a specific association, or contributions made to the trader.

[146] See E. Van Severen and E. Lievens, Online winkelen over grenzen heen: De nieuwe Verordening inzake de aanpak van ongerechtvaardigde geoblocking, D.C.C.R., 2018/2, n° 119, p. 3-16, in particular p. 13 referring to the examples of "regulated bookprices".

[147] Directive 2006/123 of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ, 2006, L 376, p. 36.

[148] Act of 10 May 2007 aiming at combating certain forms of discrimination, Belgian Official Gazette, 30 May 2007, p. 29016.

This is not a mere theoretical statement as Belgian courts already ruled that offering specific promotions or reductions to a category of consumers, according to their age[149] or their job category and localisation,[150] was not objectively justified and therefore in breach of the Belgian Discrimination Act. Such breach, in turn, was deemed an unfair commercial practice by the business from which the promotions originated.

4.2.3 Accountability and Transparency

To ensure that the enterprise, as data controller, complies with its obligations regarding the processing of personal data, it would need to ensure that any processing is compliant with the abovementioned laws dealing with consumer rights and anti-discrimination, and personal data is processed based on one of the grounds set out under Article 6 GDPR (principle of lawfulness, fairness and transparency under Article 5 (1) GDPR). The principles of data minimisation, purpose limitation and accuracy are also relevant in an AI environment and aim at ensuring that the automated processing solution is sufficiently "trained" by the enterprise to be compliant.

The data subject should be granted the possibility to be informed about the limited and specific purposes of processing, with a clear distinction between the purposes (offering a personalised price) and the means of reaching the purpose (personalisation) (purpose limitation principle under Article 5 (1) (b) GDPR).[151] Adopting and informing the consumer clearly would constitute a safeguard against a possible blurring of purposes.[152]

Transparency would require the controller to inform the consumer about the algorithms used in the framework of AI and could however be met with difficulties. The growth and complexity of AI using machine-learning, and deep-learning, can make it challenging to understand how an automated decision-making process or profiling works, and can lead to a "Blackbox phenomenon" where the AI solution would start making decisions independently, without its operator being able to understand or anticipate the rationales behind it anymore.

This complexity should however not serve as an excuse to circumvent this obligation and the controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision, especially as next to the information obligation under the GDPR, the consumer must be provided with clear and comprehensible pre-contractual information under Article VI.45 CEL. Achieving these requirements would, according to the EU Commission, improve consumer trust and welfare and empower the consumer to identify the processes and functioning of the AI, allowing them in turn to make informed decisions on their use, opt-out, or be able to check and correct any input given.[153]

Besides the transparency requirement, the quality of the automated decision is also a matter of good data governance: an AI operator should be able to "control" the behaviour of its equipment and to explain and use unbiased algorithms at all stages, which should not only be explainable to the consumer but also to all market surveillance authorities.[154]

To achieve this goal, the high-level EU expert group on AI suggests that an equipment involving AI should always be designed in a way allowing human oversight at all stages, with appropriate human involvement, before (pre-validation of data and algorithms used) and after production of the output, as well as the need for a human

[149] For instance, this has been the case for reductions offered by a glasses retailer, which went higher the older the customer was. See Court of appeal of Antwerp, 26 April 2007, and J. Stuyck, Geen goedkope brillen voor ouderen - de onverwachte invloed van de anti-discriminatiewet, Annuaire Pratiques du commerce & Concurrence, 2007, p. 478-482. Other courts have upheld the same ruling, see President of the Commercial Court of Turnhout, 7 November 2008, Annuaire Pratique du commerce & Concurrence, 2008, p. 289; President of the Commercial Court of Brussels, 17 September 2008, Annuaire Pratiques du commerce & Concurrence, 2008, p. 57; President of the Commercial Court of Brussels, 15 October 2008, Annuaire Pratiques du commerce & Concurrence, 2008, p. 272.

[150] See Court of appeal of Brussels, 4 May 2010, D.C.C.R., 2011, n°90, p. 103.

[151] See also, on the concept of personalisation, Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, adopted on 29 November 2017 and last revised on 11 April 2018. Accessed on 15 July 2020. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[152] Guidelines 05/2020 of 4 May 2020 of the EDPS, on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, consulted on 10 May 2020, n°56, p. 13.

[153] European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP)), available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0032_EN.pdf. Accessed on 28 March 2020; Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, Ethic Guidelines for Trustworthy AI, 8 April 2019, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419, consulted on 10 May 2020, p. 16.

[154] European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP)), *op cit.*, pts 13 and 14.

intervention in real time during functioning and, if needed, to deactivate the AI. This includes the decision of whether to use an AI system in a particular situation, of establishing levels of human discretion during the use of the system, or ensuring the ability to override a decision made by a system, and ensuring the ability for public enforcers to exercise oversight in line with their mandate.[155]

Data controllers should also ensure that the AI system is used as it was designed to be, undergoes training in such a way that it will only process data of quality avoiding biased results that would undermine data subject fundamental rights and lead, for instance, to an unfair discrimination between groups of individuals. The quality of data is achieved when the data is as inclusive as possible, representing different population groups, taking into account potentially vulnerable persons and groups, such as workers, women, persons with disabilities, ethnic minorities, children, consumers or other groups at risk of exclusion.[156]

Facing these challenges, it appears that a strict compliance with the data protection principles could achieve both goals. A data controller who needs to comply with transparency requirements and provide consumers with easily understandable information, allowing them to make reasoned transactional decisions, must keep an entire control of its data processing solution using automated means and be able to intervene at all stages to bring necessary improvements and corrections. This will allow the controller to assess on a permanent basis whether the processing mechanics behind the AI still satisfies data protection principles, thereby mitigating any risk of discriminating, or any harmful or unfair processing for the consumers/data subjects.

4.3 Consumer Rights and Remedies

As a third component, a better balance of power can be achieved if the consumers are granted specific rights they can easily enforce, allowing them to intervene in the decision-making that leads to personalisation or contest such decision *ex post*. GDPR and consumer laws read together seem to bring comprehensive remedies to the consumer. Their effectivity is guaranteed provided that the enterprise complies with the elements above on its own accountability obligation, and the efficient provision of information to a consumer.

4.3.1 Remedies under Consumer Law

Prior to entering an agreement, we have seen that the consumer must receive specific information, including on the personalisation of the price that they will pay for goods or services. If the consumer can demonstrate that the provided information on personalisation constitutes misleading or aggressive commercial practices, influencing their transactional decision, they can claim reimbursement of any amount paid to the enterprise while keeping the purchased good or the benefit of the services, in some instances without a judicial intervention (Article VI.38 CEL).

At the stage of conclusion of the agreement, the consumer should be granted the technical means to analyse the errors in the data they seized into the system and correct them prior to submission(Article XII.8 CEL).

After concluding the agreement online, the consumer benefits from a withdrawal right to be exercised within a 14 day period from the date of conclusion, for services, and for goods, from the date when the consumer physically takes possession of the good. This right can in principle be exercised at no costs (Article VI.47 CEL).

However, the effectiveness of such a right can be called into question in the face of AI: the withdrawal right is subject to several exceptions, and it will not apply to digital services where the consumer expressly agreed to start using it and acknowledged that by doing so, he or she would lose such right after the service is executed (Article VI.53, 13° CEL). Categories of online services are therefore excluded from this protection. Moreover, another exception denies withdrawal when the goods supplied are made according "to the consumer's

[155] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, Ethic Guidelines for Trustworthy AI, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419, consulted on 10 May 2020, p. 16.
[156] *Ibid.*, p. 11. See also Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017 and last revised on 6 February 2018. Accessed on 15 May 2020. Available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826, pp. 10-14. The data should also be up to date as "Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Inaccuracies may lead to inappropriate predictions or statements about, e.g, someone's health, credit, or insurance risk".

specifications or are clearly personalised". If not only the price, but also the good purchased is personalised by means of AI, there would be room for the enterprise to argue that this exclusion applies (Article VI.53, 3° CEL).

Also, when the transaction involves the communication of personal data, the EDPB questioned how such right would articulate with the right to withdraw consent for the processing of its personal data under Article 7 (3) GDPR, and whether after exercising such right, the consumer would maintain the possibility to effectively enforce their data subject rights under the GDPR, and what type of reimbursement, or "fair compensation"[157] would be appropriate when the "counterpart" to the goods or services is consumer's personal data.

4.3.2 Remedies under GDPR

Article 22 GDPR is construed as an exception-based prohibition to rely on automated processing, in which the data subject will always have the right to oppose such processing to the extent that this produces legal effects concerning the data subject or significantly affects him or her.[158]

"Legal effects" implies that the decision affects the data subject's legal rights, the legal status of their rights under a contract. As for the second criteria - that the processing would significantly affect the data subject - the decision must have the potential to (i) significantly affect the circumstances, behaviour or choices of the individual concerned; (ii) have a prolonged or permanent impact on the data subject and (iii) at its most extreme, lead to the exclusion or discrimination of individuals. Under any of these criteria, it appears that a data subject could successfully oppose the processing of his or her personal data. Examples in the first case would be where the use of AI will have a decisive effect on the decision to offer or not a contract to the data subject, for instance, and where the consumer accepts the offer made and created by the AI, which creates a legal obligation for the consumer to pay for the counterpart that he or she was seeking, and thus have legal effect.[159]

Outside of any legal effect, under the second criteria, the AI could be used to influence the consumer's decision, even if not related immediately to an agreement, by means of personalised advertising or other marketing techniques, where the behaviour of the consumer would be impacted and he or she would make a decision that he or she otherwise would not have taken. Unfair commercial practices could reasonably belong to this category.[160]

Then, the data subject is always granted, as a safeguard, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision (Article 22 (3) GDPR). This allows the data subject to give the data controller input, which in turn can help it improving its processing processes.

The data subject always has the right to access their personal data and see how it is processed and receive the same information about the "logic involved" (Article 15 (a), (b), (h) GDPR), and to require correction of the input if any errors or inaccuracies are found (Article 16 GDPR). If there is uncertainty about the extent to which a data controller must disclose the functioning of its algorithms, these remedies reinforce the data subject's position as he or she would have the right to access such information, and assess whether it reveals that that data controller uses

---

[157] Opinion 8/2018 of the EDPS, on the legislative package "a New Deal for Consumers", available at: https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf, p. 17-18. See also R. Robert, Peut-on payer avec ses données personnelles? - La proposition de directive "contenu numérique" introduit le ver dans le fruit, JDE, 2017, pp. 356-358. This author explains the difficulties linked to giving a precise value to personal data by, inter alia, the fact that the consumer is himself unaware that he is using personal data as a "money" in the framework of an equitable exchange, and professionals would not succeed either at determining a fair value. Moreover, the lack of clarity of some privacy policies cast doubt as to whether the collection of personal data is intended to create value in the first place.

[158] Article 22 (1) GDPR. Referring to Recital 71 GDPR, Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017 and last revised on 6 February 2018. Accessed on 15 May 2020, p. 20: "Interpreting article 22 as a prohibition rather than a right to be invoked means that individuals are automatically protected from the potential effects this type of processing may have".

[159] F. Jacques, Personnalisation des prix - Regard européen sur la pratique, R.D.T.I., n°78-79, 2020, p. 78.

[160] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017 and last revised on 6 February 2018. Accessed on 15 May 2020, p. 22: "online advertising, which increasingly relies on automated tools and involves solely automated individual decision making. In many cases, targeted advertising based on profiling will not have a significant effect on an individual but, depending on particular characteristics of the case (intrusiveness, expectations and wishes, the way the advert is delivered, using the knowledge of the vulnerabilities of the data subjects targeted)". It will have little impact generally but can have more significant effect for certain groups of society such as minority groups or vulnerable adults. A significant effect would be found here if the automated decision making results in differential pricing based on personal data or personal characteristic if, e.g, prohibitively high prices effectively barred some from certain goods or services.

criteria in breach of anti-discrimination laws for instance.[161] Moreover, if sensitive personal data under Article 9 (1) GDPR requiring explicit consent is processed, the data controller should take suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, and automated processing can only take place if these requirements are satisfied.[162] As this type of data is obtained through consent, the data subject can withdraw their consent at any time (Article 7 (3) GDPR).

The collected data itself should be limited to elements that are relevant and should not create any discrimination in view of personalisation, and allow the data subject to make a correct use of its rectification right to ensure that such data is accurate.[163] This would, in turn, ensure that the data minimisation principle and the quality of that data are complied with.

4.4 Synergies Between Consumer Law and Data Protection

Provided that, under the applicable rules, both the enterprise, provides a transparent and consumer-friendly environment, and the consumers are vested with effective rights, the legal arsenal in place could already serve as a good base facing the growing use of automated processing means such as AI. This is best achieved not through a legislative change, but based on the correct training, and willingness of the stakeholders to effectively comply with the rules in place, allowing the emergence of a renewed B2C model embracing new technologies. The consumer gains trust in entering into transactions using automated systems if it can effectively enforce its rights that give control over the personal data, data that it is willing to disclose and for which they can have an influence on processing by using their right to corrections. This however supposes that the enterprise, on their side, correctly provides information about processing knowing that incorrect or misleading information, in breach of data protection laws, could constitute an unfair commercial practice subject to sanctions.

5. Conclusion

In this contribution, we have seen that new challenges brought by modern marketing techniques could be faced using a technology-neutral legislation and pleading for an effective and combined reading of the rules under both consumer and privacy laws.

Further legislative efforts should be made to ensure that the rules covering commercial communication subject all medias to the same rules, and make the identifiability requirement for a "promotion" applicable in broader terms, that is covering economic or non-economic purposes. This would allow consumers to understand the intent behind the numerous communications that they receive and prevent them from undue influence on their decision-making process, be it for an economic transaction or a social activity, with a sufficiently critical mind taking the average consumer criterion into account.

Personalisation, with or without the use of AI, to facilitate the conclusion of an agreement will be best captured by law not through legislative change but if the existing rules can be approached with a flexible application of consumer laws, on the one hand, and a reasoned approach towards privacy laws, taking into account consumer's fundamental rights as embodied under anti-discrimination laws.

The existing consumer laws, and the upcoming changes brought by the Omnibus Directive, can be applied and enforced in such a way that not only the price, but the personalisation of the entire transactional process can be captured under the rules applicable to unfair commercial practices.

Under privacy laws, the existing GDPR rules compels the enterprise to carefully assess the correct use of personalisation and the use of technology, materialised by a correct information to the consumer, in a manner allowing the consumer to understand their rights, whether personalisation is made using consent or legitimate interests as a legal basis. Moreover, a strict compliance with the data protection principles and sufficient transparency on the means of processing used will help the enterprise achieve better results in terms of

[161] F. Jacques, Personnalisation des prix - Regard européen sur la pratique, R.D.T.I., n°78-79, 2020, p. 67 quoting L. Drechler and J.-C. Benito Sanchez, "The Price is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms", European Journal of Law and Technology, 2018/19 (3), p. 12.
[162] Article 9 (2) (a) GDPR read with article 22 (4) GDPR.
[163] Article 16 GDPR.

personalisation, with the collaboration of the consumer controlling its data, which in turn will allow for an improved delivery of goods or services.

What then about other applicable laws safeguarding the consumer's fundamental rights or further technological evolution? The same rules can be seen as a possible safety net. The way that the "general norm" under unfair commercial practices is interpreted under EU and Belgian law is broad enough to be "future proof".[164] A judge or a regulator applying this norm will have to acknowledge that any stakeholder involved with the concept of personalisation and the use of AI has to comply with the rules of GDPR as well as anti-discrimination laws. Even without breaching the law, any personalisation practice could be deemed contrary to professional diligence or distort the economic behaviour of a consumer, as personalisation, whether or not through the use of AI, is susceptible to influence a consumer's transactional decisions.

This pleads for a reviewed approach at both the EU and Belgian level where the relevant unfair competition and privacy stakeholders should interact and adopt common solutions and guidelines to ensure an appropriate application of these rules. This will, in turn, help achieve a better balance of power on both sides. The consumer/data subject will be correctly informed of the promotional and personalised nature of the message conveyed to them and enforce rights to prevent any misuse of personal data threatening their fundamental rights or giving them the choice not to be subject to personalisation or automated decision-making, allowing them to gain trust in the use of such new technologies. The enterprise/data controller willing to achieve a future-facing market position taking a consumer-centric approach into account, will need to have the appropriate safeguards in place ensuring that they maintain control over their personalised communication and automated-processes, which should remain identifiable and understandable at all time, knowing that breaches could expose them to regulatory or consumer enforcement at both unfair competition and privacy levels.

[164] N. Van Eijk, C. J. Van Hoofnagle and E. Kannekens, Unfair Commercial Practices: A Complementary Approach to Privacy Protection, E.D.P.L., n°3, 2017, p. 325-327.