UCLouvain

Faculty of Law and Criminology

Vulnerability and AI-based technologies: European protection of vulnerable consumers in the digital market

Graduating student : **Claudia LANZA**

Supervisor : **Stéphanie FRANCQ**
Co-supervisor : **Marc FALLON**

ACADEMIC YEAR 2022-2023
Master's Degree Program in Law with professional focus: European Law

To the sacrifices of my mom,
and the intensity of her love

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

Abstract

The concept of vulnerability holds an important, yet often overlooked role. With a digital market governed by new technologies, vulnerability has become a source of exploitation and algorithmic discrimination. This study aims to determine how AI-based technologies exacerbate pre-existing vulnerabilities or create new ones, with the objective of establishing if European law grants protection to vulnerable consumers and to what extent. The core revolves around the negative impact that AI-deriving technologies can have on individuals. The analysis rests on the comparison between vulnerability under European consumer law and European Acts implementing digital decade. On this ground, this work proposes a newer and wider perspective centred on vulnerability and addresses potential solutions to tackle legal gaps within this framework.

Contents

Introduction

The concept of vulnerability holds an important, yet often overlooked role. On the contrary, the digital market has always been a crucial point of interest of the European Union. It is precisely in a digital era where technologies grow enormously and transactions are predominantly online that vulnerability becomes the breeding ground for exploitation techniques.

This work intends to focus on how the digital technologies exacerbate pre-existing vulnerabilities or create new ones, in order to assess if vulnerable consumers are granted sufficient protection by the European law. The main field of research are European consumer law and the European Acts implementing the digital decade. For this purpose, this study is composed of four chapters: the first chapter analyses the current notion of vulnerability within Consumer law, identifies what are these new technologies and their risks to vulnerable consumers. The second chapter proposes a new perspective on vulnerability to tackle these risks. The third chapter examines in detail the legal framework in the matter, in particular the Proposal for an Artificial Intelligence Act (AI Act). The last chapter contemplates several remarks that emerge from the critical analysis of the regulatory framework, therefore suggesting five solutions that would fill the legal gaps in the matter.

This work adopts a problem-based approach: it first evaluates the insufficient guarantees to the vulnerable, to then build five proposals to address the problem. The results are exposed in detail in the final chapter of this thesis.

As a premise, all references to "advertising" refer to advertising specifically supported by an AI-based technology. Correspondingly, all references to "online choice structure" or "surface design", refer to data-driven adjustments of online choice structures or surface designs made by traders.

Chapter 1

Vulnerable persons

In the first chapter the focus lies on the notion of vulnerable persons within Consumer law. For a better understanding, an in-depth analysis of the consumer concept will be conducted, to clearly identify the differences between the latter and the vulnerable. Furthermore, the chapter highlights the necessity of the co-legislators to identify and protect the more fragile individuals among consumers.

1.1 General insight

One of the main competences of the European Union is to guarantee a high level of consumer protection.[1] It does so by promoting a consumer's public policy, which must be observed in all fields and actions that the Union treats.[2] It is thus a transversal objective both for the Union and its Member States, as it is a matter of shared competences.[3] It is of such great importance that it is now considered as being part of the overriding reasons of public interest.[4]

In the contractual relationship, the consumer is always considered as the weaker party. In fact, the consumer is defined as the one having a significantly weaker position *vis-à-vis* the trader, due to lack of bargaining power[5] and uneven access to information.[6] As a result, the legislator has created different sources of protection regimes dedicated to consumers.

---

[1] Art. 169 TFEU. See also B.B. DUIVENVOORDE, *The consumer benchmarks in the Unfair Commercial Practices Directive*, Amsterdam, Springer, vol. 5, 2015, p. 17.
[2] Art. 12 TFEU.
[3] Art. 4 (2) TFEU.
[4] C.J.E.C., case *Corsten*, 3 October 2000, C-58/98, EU:C:2000:527, para. 38.
[5] N. HELBERGER *et al.*, « Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability », *Journal of Consumer Policy,* 175-200, 2022, p. 177.
[6] A. WIEWIOROWSKA-DOMAGALSKA, « Contribution to growth. Legal Aspects of Protecting European Consumers, Study for the Committee on the Internal Market and Consumer Protection », Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 79.

Consumer protection is arranged *via* information:[7] if the consumer is informed, he is protected.[8] That was firstly indirectly affirmed in the notorious caselaw Cassis de Dijon[9] where the European Court of Justice (hereinafter ECJ) stated that "*it is a simple matter to ensure that suitable information is conveyed to the purchaser by requiring the display of an indication of origin and of the alcohol content on the packaging of products."* The consumer needs to be informed in order to be protected.[10] The idea behind it is that a well-informed person can choose wisely. A good example is the Consumer Rights Directive*;* sellers should ensure that consumers are not misled by providing them with a set of information.[11] Consumer law is thus characterized by a precontractual phase focused on ensuring adequate consumer information,[12] reverse the presumption of misinformation and to empower consumers by elevating them as experts.

1.1.1 Information overload

Information overload is an important element to consider when trying to understand consumer protection. Studies have shown that it is not clear for consumers to make a rational decision when facing a great deal of information.[13] Some studies also show that consumers are likely to make poorer decisions when given more choice.[14] This is especially true when it concerns the vulnerable.

The increase of the aggressive sales practices, also empowered by new technologies, contributes to highlight consumer's vulnerability. This became more evident with the continuous evolution of digital technologies, as the specificities of distance contracts

---

[7] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *Rethinking EU consumer law*, Routledge, New York, 2018, pp. 7, 11 and 95.
[8] P. SICILIANI, C. RIEFA, H. GAMPER, *Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement*, Oxford, Hart Publishing, p. 18, partially available on Google Scholar.
[9] C.J.E.C., case *Cassis de Dijon*, 20 February 1979, C-120/78, EU:C:1979:42, para. 13.
[10] B.B. DUIVENVOORDE, *op. cit.*, pp. 13 to 17.
[11] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, *O.J.*, L 304, 22 November 2011.
[12] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *op. cit.,* pp. 96 to 106.
[13] C. RIEFA, « Protecting vulnerable consumers in the digital single market », *European Business Law Review,* 2022, pp. 17 and 96.
[14] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *op. cit.,* pp. 33 to 35, 97-98.

have justified the necessity of more robust information obligations across various types of contracts.[15] In fact, there were many situations where the trader did put the information at the consumer disposal but his active behaviour was needed in order to concretely find this information. But for individuals belonging to lower socio-economic groups is more likely to face decisions of higher uncertainty and require superior cognitive efforts to find that information[16]; therefore they are also less likely to possess the necessary skills to assess such complex contracts. The European Parliament confirmed this vision, declaring that concentrating protection mechanisms on information "*may be insufficient to protect vulnerable consumers, since their vulnerability may originate from their difficulty in accessing or assessing the information given to them*".[17]

1.2 Vulnerability under European consumer law

What emerges so far is that consumers are already somewhat vulnerable due to their limited access to information and negotiating power.

The concept of vulnerability was born while drafting one of the main instruments within European consumer law, the *Unfair Commercial Practices Directive*[18] (henceforth, UCPD). This Directive entered into force in 2005, with the underlying premise of prospering the digital market.[19] It was indeed the premise of all the instruments in the context of consumers protection of that period[20], and still is.[21]

---

15 B. GOFFAUX, « Le devoir général d'information dans le droit belge de la consommation », *D.C.C.R.*, 2013, pp. 253 et seq.

16 C. RIEFA, *op. cit.,* p. 5. R.P. HILL, E. SHARMA, « Consumer vulnerability », *Journal of Consumer Psychology,* 30/3, pp. 551 to 570.

17 European Parliament, « Resolution of 22 May 2012 on a Strategy to Strengthening the Rights of Vulnerable consumers », *O.J.,* CE 264/11, 13 September 2013, para. 9.

18 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, *O.J.,* L 149/22, 11 June 2005.

19 C. RIEFA, *op. cit.*, p. 12.

20 See, for example, the *Distance Selling Directive 97/7* and the *Doorstep Selling Directive 85/577*, however both no longer in force.

21 Current instruments in consumer policy all share the same legal basis which is article 114 TFEU.

In order to achieve that goal, the European legislator introduced the idea of a "*laissez-faire*",[22] basically allowing traders act in their own interests as long as they informed consumers about their actions. The instruments in the field aimed at marginalize only some practices or behaviour that could be exceptionally prejudicial for the consumers, therefore unacceptable. This Directive works hand in hand with the *Directive on Consumer Rights*, wherein appears a list of information that the traders must provide to the consumers for them to be granted protection.

The *rationalis* behind this approach is that if the consumer is properly informed, he would be less likely to take a regrettable or unfavourable decision; The consumer is empowered through information.

The application of consumer protection in concrete cases led the European Court of Justice to enunciate the milestone of interpretation in consumer law. In the *Gut Springerheide* caselaw the Court stated and defined the average consumer standard requirements as an "*informed, observant and reasonably circumspect person*". [23]

The starting point to establish whether the protection could or could not be granted was indeed to analyse if the consumer had been given the possibility to properly inform himself, observe the product and its related advantages or risks and subsequently decide whether proceed with the purchase or not. This concept empowered the average consumer to take an active role in making a decision exempt from mistakes: an active role was granted to consumers.[24]

The great novelty of the UCPD was to introduce for the first time a normative definition of this concept: because of its degree of harmonization[25] and its broad field of application, this led to a big change into the interpretation and the application of this concept for the national Courts of Member States.[26]

---

[22] N. HELBERGER *et al., op. cit.,* p. 196.
[23] C.J.E.C., case *Gut Springerheide*, 16 July 1998, C-210/96, EU:C:1998:369, para. 31.
[24] N. HELBERGER *et al.*, *op. cit.,* p. 178.
[25] It has, indeed, a total harmonization character, which means that the matter is settled exhaustively by the European Union, impeaching its Member States to expand or decrease the level of protection settled by the act.
[26] B.B. DUIVENVOORDE, *op. cit.*, p. 14.

Additionally, it introduced for the first time the concept of vulnerable consumers. In its article 5 (3), the UCPD expressly refers to consumers in vulnerable conditions, namely individuals with physical or mental infirmity, underaged or elderly persons. The average consumer standard is also applicable, being the consumer of reference the "average member" of this very group. Thus, vulnerable consumer and average consumer benchmarks are two intertwined concepts. Article 5 reads as follows:

> " *1. Unfair commercial practices shall be prohibited.*
>
> *2. A commercial practice shall be unfair if:*
>
> *(a) it is contrary to the requirements of professional diligence,*
>
> *and*
>
> *(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the* ***average member of the group*** *when a commercial practice is directed to a particular group of consumers.*
>
> *3. Commercial practices which are likely to materially distort the economic behaviour only of a* ***clearly identifiable group*** *of consumers who are* ***particularly vulnerable*** *to the practice or the underlying product because of their* ***mental or physical infirmity****,* ***age*** *or* ***credulity*** *in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group. This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or statements which are not meant to be taken literally.* "[27]

Evidently, vulnerability under the UCPD refers to the internal and intrinsic characteristics of the consumer.[28] There are no references to the consequences of a particular practice that could render someone vulnerable[29], nor there are references to external factors that could lead the consumer to a status of vulnerability with no relationship

[27] Art. 5 (3) UCPD.
[28] N. HELBERGER *et al.*, *op. cit.,* p. 178.
[29] C. RIEFA, *op. cit.,* p. 6.

with credulity or age or handicap.[30] The role of this concept is therefore very limited but one exception in this regard is worth to be addressed: in the financial field, more specifically in the matter of international loans, the average consumer standard used by the European Court is reinforced. In the *Kásler* case the judge indeed admits that the consumer must be granted a stronger protection. It thus completes the consumer standard with an additional requirement: a deep understanding of the consequences of the loan. As it is in fact insufficient for the consumer to be reasonably well-informed, observant and circumspect, he must also be capable to understand the consequences of such transaction.[31]

It is very unfortunate to observe that on the occasion of the 2017 REFIT, the UCPD has remained intact with respect to the definition of vulnerability.[32] Moreover, the 2019 *Directive as regards the better enforcement and modernization of Union consumer protection rules*[33] (the so-called "Modernisation Directive" or "Omnibus Directive") states in its Recital 54 that some particularly aggressive or misleading marketing or selling practices can put consumers under pressure, especially because these practices often target elderly or other vulnerable persons. The Commission does not specify who are these "other" vulnerable persons, but because it did not modify article 5 (3) of the UCPD, it is logical to assume that it refers to the definition of vulnerability stated as such in the Unfair Commercial Practices Directive. However, it did keep a glimmer for the change and the enlargement of the definition. It is contradictory for the Commission to have missed such opportunity since the primary aim of the 2017 REFIT was to revise all consumer protection rules in order to ensure their efficiency and effectiveness considering the newest development of the digital market.[34]

---

[30] *Ibidem,* p. 6: "*As a result, the low-income consumer is not normally considered vulnerable in the context of the UCPD. Payment problems or poverty are public law issues and find responses under welfare law, not consumer law*."

[31] C.J., case *Kásler,* 30 April 2014, C-26/13, EU:C:2014:282, para. 60.

[32] Study for the Fitness Check of EU consumer and marketing Law - Final report Part 1 - Main report, European Commission, DS-02-17-420, 2017.

[33] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, *O.J.,* L 328/7, 18 December 2019.

[34] *Ibidem,* Recital 17.

Furthermore, the same UCPD hints in its Recital 19 that the definition of vulnerable persons may be non-exhaustive[35]; it does so by formulating its recital, which states the characteristics of vulnerability preceded by the prepositional phrase "such as".[36]

However, in 2021, the Commission updated the *Guidelines concerning unfair business-to-consumer (B2C) commercial practices in the internal market*, stating precisely that vulnerable characteristics are not limited to the one laid down in article 5 (3).[37] As clarified by the Commission itself, vulnerability on the contrary has different dimensions and can change according to different situations. The average and vulnerable consumer standards can be assessed differently with respect to the specific circumstances of the case. While the update was positively received, it does lead to legal uncertainty. Because guidance is not legally binding,[38] it is not clear how the modulation of these concepts, and in particular the vulnerable one, can be applied by domestic Courts. The concept lacks clear boundaries.

As previously said, this would have been the perfect occasion to provide the UCPD with a span-new conception, adapted to the evolution of the marketing strategies.

1.3 New technologies: new risks

The estimated growth of global AI market is almost 40% each year[39], which echoes how important this sector is in the economy and how increasingly will grow. These technologies are employed to support decisions in a variety of domains as they enable labour cost cutting, manage resources more efficiently[40], while handling larger databases and easing employees' workload.

---

35 B.B. DUIVENVOORDE, *op. cit.*, pp. 21, 24 to 27.

36 "*Where certain characteristics such as age, physical or mental infirmity or credulity make consumers particularly susceptible to a commercial practice or to the underlying product and the economic behaviour only of such consumers is likely to be distorted.* [...]"

37 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *O.J.*, C 526/1, 29 December 2021, p. 99.

38 B.B. DUIVENVOORDE, *op. cit.,* p. 16.

39 14th annual report of the Future Today Institute on Strategic trends that will influence business, government, education, media and society in the coming year, 2021, p. 8.

40 A. MONARCHA-MATLAK, « Automated decision-making in public administration », *Elsevier B.V,* 192/2021, p. 2078.

Artificial Intelligence (AI) is a branch of computer science that is progressively being employed in several fields, both in private and public sectors.[41] In reality, AI is the broad science, that many other technologies and software derive from and that are empowered by it. One of these AI-derived technologies is Machine Learning (ML), the most employed technology in the digital market.[42]

In fact, AI is the discipline that supports the creation of "intelligent machines"[43] but it is actually ML that allows these machines to learn from data. In other words, ML is a subset of AI; it enables machines to learn from historical data, while AI uses the algorithms created by the ML to simulate human intelligence. Although they might appear to be the same, they very much differ. For ease of reading, this work will employ the word "AI" to describe any AI-deriving technology, may it be ML or another branch, although it will mostly refer to ML, as it is the automated process *par excellence.*[44]

Deriving technologies employ the use of different algorithms and the difference stands in their nature. There are algorithms trained with structural data, [45] meaning that they learn from historical data (hence already existing information), and unstructured algorithms capable of handling unknown circumstances, and solve complex tasks that were traditionally solved by humans. Predictions and automation are some of the deployed goals, capable of performing human cognitive functions. The added-value is not only the rapidity on which AI-based technologies[46] can, for instance, predict consumers choices or adjust platform settings[47] to improve surveillance advertisings, but is also that they can structure the collected data like humans. To name but one, AI can find hidden patterns for grouping consumers by their purchasing patterns.[48]

---

[41] *Ibidem.*
[42] F. ZUIDERVEEN BORGESIUS, *Discrimination, artificial intelligence and algorithmic decision-making*, Strasbourg, Directorate General of Democracy, 2018, p. 12.
[43] *Ibidem.*
[44] 13th annual report of the Future Today Institute on Strategic trends that will influence business, government, education, media and society in the coming year, 2020, p. 27.
[45] A. MONARCHA-MATLAK*, op. cit.,* p. 2079.
[46] In the interest of clarity, I will use "AI-based technologies/systems", "AI-empowered technologies/systems", "AI-derived technologies/systems" as synonyms.
[47] F. MARTY, « Plateformes numériques, algorithmes et discrimination », *Revue de l'OFCE*, 2019/4 164, p. 48.
[48] F. ZUIDERVEEN BORGESIUS, *op. cit.,* p. 14.

Despite this short attempt to give a small insight on what AI-based technologies are and how they are implicated daily, the matter is considerably more complex. Wider explanations are left to the discretion of the reader.

AI-based technologies systems allow companies to collect and use a large amount of data on users' behaviour and preferences in order to transform them in reusable information for commercial purposes, *via* personalized approaches.[49] Hence, employment of AI software can be a very enriching asset, but it is important to highlight that it can lead to several risks at different levels. Regardless the type of AI-empowered software, the question resides in the input of data that the algorithm is trained on, that may spread discrimination.[50] This phenomenon takes the name of "algorithmic discrimination".[51] Below reported the practical implications of this phenomenon:

- Biased data collection:

AI may use historical datasets, i.e. existing information.[52] According to this data, an algorithm will be generated. The training data can perform a discriminatory output because it represents some historical biased decisions.[53] AI Amazon tool provides a good example to illustrate this point: it was projected for the purpose of rating job applicants and mechanize the search for the most talented candidates. Amazon AI system was trained with the past ten years of recruitment pattern, which reflected the man dominance in the sector.[54] In 2015 Amazon programmers found that all resumes containing the word "women" (may it be for the gender of the applicant or the name of the college the person graduated to) were excluded. The algorithm *in casu* reflected the male predominance in that sector.

---

[49] C. RIEFA, *op. cit.,* p. 15.
[50] Room Document of the European Data Protection Supervisor (EDPS) for the 38th International Conference of Data Protection and Privacy Commissioners, 2016, p. 4, available on https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en
[51] C. ARGELICH-COMELLES, *Inteligencia Artificial y tratamiento legal de la discriminación algorítmica en los online marketplaces de consumo*, thesis, Universidad Autónoma de Madrid, 2022, p. 7.
[52] F. ZUIDERVEEN BORGESIUS, *op. cit.,* p. 17.
[53] *Ibidem,* p. 9 and 18.
[54] A. A. KODIYAN, « An overview of ethical issues in using AI systems in hiring with a case study of Amazon's AI based hiring tool », *Researchgate Preprint*, 2019, pp. 1-2.

- Biased feature selection:

The feature selection refers to categories of data. When a company or an organization wants to use AI for automated prediction, it needs to insert simplified words that may capture the prediction goal.[55] For instance, if the goal is to identify what category of consumers is most likely to be interested in the purchase of an online course, the institution may want to select individuals with some sort of educational background. The institution could then focus only on certain features in order to get potential interested individuals. By selecting these characteristics, the institution could involuntarily establish biases against other groups, e.g. individuals with economic difficulties who may have not had the possibility of pursuing an academic career.[56] This type of concern has an increased impact over the most susceptible categories of consumers: if entering the words "reproductive health" or "mental health", consumers in a certain vulnerable situation may be especially affected.[57]

- Predictive analytics

The use of predictive analytics' technique can similarly be source of discrimination[58], that is because predictions that are supposed to update the existing data, generate an algorithm that will then be used to collect future data and generate another algorithm. Hence some authors call it "algorithms that influence algorithms"[59]: over time, any bias

[55] F. ZUIDERVEEN BORGESIUS, *op. cit.,* p. 20.
[56] F. ZUIDERVEEN BORGESIUS, *op. cit.,* pp. 17 and 20.
[57] Stretching this hypothesis to its more extended risks, this concern has already been addressed in very recent caselaw. In the context of public administration, the Dutch government employed AI systems to create risk profiles of childcare benefits seekers. The words selected to perform this goal were "'foreign sounding names" and "dual nationality"; on this basis, the algorithm categorized thousands of individuals, who were erroneously accused of fraudulent demands. The Dutch Data Protection Authority affirmed that the algorithm used in the performance of this automated prediction was indeed biased. For further reading: https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=741047&l=en
[58] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, « BigData: discrimination in data-supported decision making », 2018, p. 13, available on https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making
[59] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, « Artificial Intelligence for Europe », COM (2018), 237 final, 25 April 2018.

in the original commands will only be reinforced through the generation of its subsequent.[60] In software engineering, this method is known as feedback loop.[61]

- Intentional discrimination

Until now the issue regarded the unvoluntary processing of biased data. The idea in this segment is to reiterate that companies may intentionally use data for discrimination purposes, with the aim of generating biased results.[62] For instance, the US Target Corporation used a prediction score to identify female consumers who were at the beginning of their pregnancy; they aimed at targeting pregnant women with specific and necessary products for the entire duration of the pregnancy and beyond.[63] The US retailer used this information to increase its marketing strategies. The given example shows that, if companies can have a precise insight about consumers' needs, they might exploit[64] this information in their favour[65], e.g. showing to consumers in vulnerable situations products and goods that would allegedly help their conditions, with a high price.[66] The vulnerable may buy or engage in something that is out of his range and would not have purchased without the insidious input of the company. Consumer behaviour is thus altered.

- Sensitive data processing

The techniques above mentioned are based on demographic and geographic data, as well as behavioural characteristics, among others. In general, their accuracy is improved through the collection of consumers data on age, ethnicity, gender, economic status.

The resulted overall risk in algorithmic discrimination is translated, when confronting consumers, into two main concerns: automated-decisions making and surveillance

[60] Room Document of the European Data Protection Supervisor (EDPS) for the 38th International Conference of Data Protection and Privacy Commissioners, *op. cit*., p. 4.
[61] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, « Bias in Algorithms – Artificial Intelligence and Discrimination », *Publications Office*, 2022, pp. 8-9.
[62] F. ZUIDERVEEN BORGESIUS, *op. cit.,* p. 22.
[63] *Ibidem.*
[64] N. HELBERGER *et al.*, *op. cit.,* p. 182.
[65] *Ibidem,* p. 196.
[66] F. MARTY, *op. cit.,* p. 61.

advertisings. Algorithmic discrimination is the source, automated-decisions and surveillance advertisings are the manifestation of it.

Historical data is monitored and studied by AI-based technologies in order to deliver the right message to the right customer. Customers behaviour is observed in detail, from the purchases history to the way one navigates into different websites pages: the so-called behavioural pattern.[67] AI is also used to analyse customers sentiment. It is from the opinions that the user shares on social media or the feedback that a client leaves on a platform providing services, that the analysis will be based on. Once the interests or the unsatisfaction of a certain matter are determined, the "right" message to the "right" individual will be delivered. All the above reflects one's digital identity.

With AI, advertisers can thus go beyond simple demographic data: observance of customers sentiment and behaviour permits the consent to personalized advertisings, also known as targeted advertisings or surveillance advertisings.[68] They show a certain ad to a certain individual who, according to his digital identity, should be more interested in that content than another customer. Surveillance advertisings become more powerful – and more dangerous to vulnerable people[69] – with real-time bidding (RTB),[70] a technique that allows to dynamically modify an advertisement.

AI-based technologies put the trader in an especially powerful position, thus creating a bigger inequality of power between the latter and the consumer. All these concerns are even more real and concrete when it comes to persons with vulnerable conditions or situations. Researches[71] have shown that this category of people prefers AI-based technologies interactions to human interactions. That is because of psychological effects naturally inducted in one's mind when interchanging with an AI agent, as they are software programs conceived to interact with its environment avoiding the fear of

---

[67] F. MARTY, *op. cit.,* p. 54.
[68] PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY, « The impact of the General Data Protection Regulation (GDPR) on artificial intelligence », *European Parliamentary Research Service*, PE 641.530, 2020, p. 15.
[69] C. RIEFA, *op. cit.,* p. 15.
[70] F. MARTY, *op. cit.,* p. 60.
[71] V. PITARDI *et al.*, « Service Robots, Agency, and Embarrassing Service Encounters », *Journal of Service Management,* vol. 33/2, 2022, pp. 389 to 414 and W-H. SUNNY TSAI *et al.,* « Human versus chatbot: Understanding the role of emotion in health marketing communication for vaccines », *Wiley,* 2021, vol. 38/12, , p. 2378.

anticipated social devaluation as they are conceived to be more kind in the interaction not being genuine. [72] Customer services' chatbot might collect all the information given by the consumer during the conversation and reuse it for the purposes listed above.

The idea that AI-based technologies pose serious risks for vulnerable people is reinforced by another empirical study[73], that has shown that any person is more prone to oversharing and disclosing more information about their vulnerabilities when interacting with a non-human agent. That is because intelligent agents establish a more confidential space compared to the one created by humans.[74] All these theories are based on the assumption that AI technologies have less brain than humans[75]; this consideration corroborates the concern about AI-associated risks on people with vulnerable conditions and situations.[76]

[72] However (although not relevant in this work, it is important specify the following) this effect ceases to exist with the anthropomorphizing of AI. There is indeed a mechanism by virtue of which AI machines take the guise of human beings, hence with human characteristics. Emotional and intellectual capacities are attributed to the non-human agent, therefore they will endure the same process of anticipated social devaluation as they were human agents. For further reading: N. MOZAFARI, M. HAMMERSCHMIDT, W.H. WEIGER, « AI and the vulnerable », 2022, available on ResearchGate.

[73] W-H. SUNNY TSAI *et al., op. cit.,* p. 2381.

[74] V. PITARDI *et al, op. cit.*, p. 406.

[75] H.M. GRAY, K. GRAY, D.M. WEGNER, « Dimensions of mind perception », *Science*, 315(5812), 2007, p. 619.

[76] For further reading: N. MOZAFARI, M. HAMMERSCHMIDT, W.H. WEIGER, « AI and the vulnerable », 2022, available on ResearchGate.

Chapter 2

A new approach to vulnerability

Technologies are, as pointed out in the previous chapter, a driving factor to vulnerabilities.[77] In view of the latest development of the digital market, the concept of vulnerability as analysed in the beginning of this work may not grant sufficient safeguards. As a result, UCPD's conception of vulnerability seems to be overtaken. This chapter provides an explanation of this statement, as well as a new perspective on vulnerability adapted to the latest technologies. This work argues for a more universal conception[78], relying on different behavioural and empirical studies that some authors[79] led throughout the years.

2.1 The necessity of a broader conception

The basis for this new understanding is based on three main pillars.

Primo, the current conception appears to be a fictitious notion derived from another fictitious standard (the average consumer benchmark), that has not been tried in concrete cases due to lack of national caselaw specifically addressing the matter.[80] This causes a great status of legal uncertainty as it is not possible to ascertain whether this standard effectively protects individuals *in casu* or not, therefore creating a more favourable frame to abandon this conception and adopting a new one.

The second ground is the Commission's recognition of a stronger understanding of

[77] C. RIEFA, *op. cit.*, p. 13.

[78] N. HELBERGER *et al., op. cit.,* p. 183.

[79] More specifically, I refer to the following authors: Helberger, Duivenvoorde, Cartwright. They all studied vulnerability under a different perspective. I extrapolated their main ideas and I based some of my considerations out of their studies. Their enriching researches provided this work with a strong background, from which concrete suggestions and critics have been redacted.

[80] Only few caselaw specifically addressed the matter: *Xenalis dimagranti*, Italian case, n° PS6980 available on https://www.quotidianosanita.it/allegati/allegato8206529.pdf, *Link*, Hungarian case, n° Vj-5/2011/73, available on https://www.gvh.hu/dontesek/versenyhivatali_dontesek/dontesek_2011/7467_hu_vj-5201173, and *Pro-activ aiuta a mantenere il colesterolo,* Italian case, n° PS649 available on https://e-justice.europa.eu/caseDetails.do?idTaxonomy=6558&idCountry=15&plang=en.

weakness.[81] In its communication[82], the Commission indeed recognizes that a vulnerable consumer is someone who:

> "*as a result of* ***socio-demographic*** *characteristics,* ***behavioural*** *characteristics,* ***personal situation****, or* ***market environment****:*
>
> - *Is at higher risk of experiencing negative outcomes in the market;*
> - *Has limited ability to maximize their well-being;*
> - *Has difficulty in obtaining or assimilating information;*
> - *Is less able to buy, choose or access suitable products; or*
> - *Is more susceptible to certain marketing practices."*

This definition hints that, in order to assess vulnerability, one must look to the position of the individual in question *vis-à-vis* the other party. Based on this description, it is entirely conceivable to perceive vulnerability emerging from external factors, and not solely arising from internal and intrinsic aspects. The factors proposed by the Commission are indeed situational, which implicitly means that they may or may not persist over time.

For instance, socio-demographic characteristics can change when relocating, as the address constitutes a collected data that will subsequently show different advertisings at different prices to different persons but of the same product (price discrimination).[83] Besides, personal situations are strictly related to economic circumstances, where for example one's willingness to pay (WTP)[84] fluctuates with the alteration of one's actual capacity to pay. Consumers can thus be vulnerable in one situation and not in another. The Commission justified this new consideration based on the below public survey results on vulnerability.

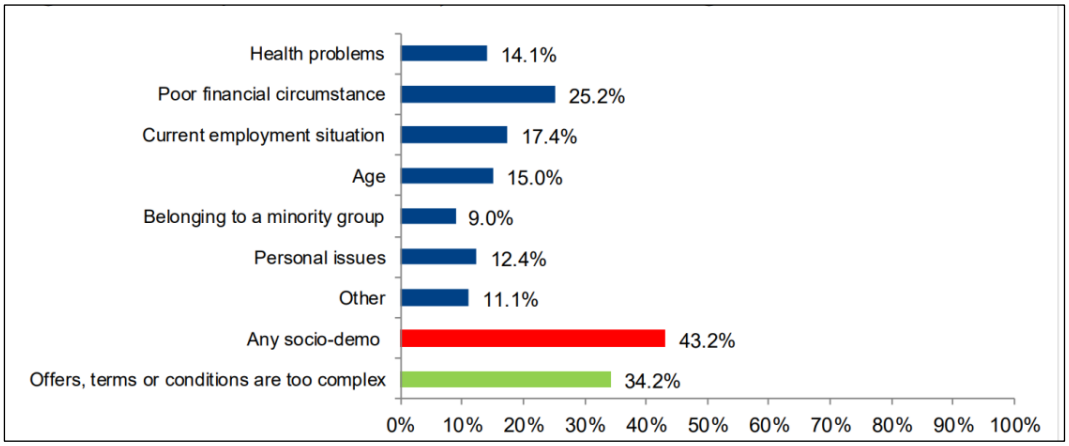
---

[81] To avoid repetition and ensure variety, I will use "vulnerability", "weakness" and "disadvantage" as synonyms, although in researches field these concepts reveal different assumptions than the vulnerability as such. For further explanations see D. LECZYKIEWICZ, S. WHEATERILL, *The Image of the Consumer in EU Law: Legislation, Free Movement and Competition Law,* Bloomsbury Publishing, London, 2018.

[82] Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union, *Publications Office*, 2016, p. 5.

[83] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit.*, p. 102.

[84] C. RIEFA, *op. cit.,* p. 22.



Source: European Parliamentary Research Service, available on https://www.europarl.europa.eu/Reg/Data/etudes/BRIE/2021/EPRS_BRI(2021)690619_EN.pdf

Figure 2.1: Self-reported vulnerability in the EU during the survey

Concurring factors can lead to different types of vulnerabilities:

- Temporary vulnerability

From the Commission's perspective it also emerges that vulnerability can be temporary.[85] While the age factor can undoubtedly change, physical and mental health as indicated in the UCPD are rather persistent in time, thus permanently affecting someone. However, it is interesting to indicate that – at least for some – not all physical conditions are permanent. Indeed, a differentiation must be established between physical permanent infirmity (e.g. a chronic illness), and physical temporary infirmity (e.g. the consequences of a small accident). Hence, individual characteristics conceived as permanent attributes are not the only sources of disadvantage.[86]

- Situational vulnerability

The Commission's new understanding of vulnerability, as previously explained, reveals a new perspective: someone can also become vulnerable *vis-à-vis* someone

[85] N. HELBERGER *et al.*, *op. cit.,* p. 184.
[86] *Ibidem.*

else[87], i.e. power imbalance between two parties. At the end, this idea reflects ***unus et idem*** the definition of a consumer as such, who is indeed the weaker party in the contract. What was just described is the third pilar that this work will be based on: everyone can become a vulnerable individual.[88] On the digital market, people in vulnerable positions are no exception. Rather, they are the norm.[89]

- Dispositional vulnerability

Weakness must not be intended from the sole perspective of someone with "limited abilities", but also from the "degree of exposure" to certain commercial practices and its consequences.[90] The degree of exposure on digital market appears to be constant. In fact, everyone is potentially vulnerable. The terminology used in research fields are "occurrent" and "dispositional"[91], where the first indicates someone's already experiencing vulnerability and the latter indicates the potential of someone to become vulnerable. The idea is that in the digital era, the use of data-driven systems is not only able to identify occurrent vulnerability, but also and especially are capable of learning how customers – under specific circumstances – can be rendered vulnerable.

A clear example of dispositional vulnerability can be related to the collection of data for profiling purposes. Profiling is "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".*[92] When a user employs a digital service, the latter holds all data to create a persuasion profile tailor-made for that costumer. Although the digital service may not use it immediately, once the persuasion profile has been established, the collected data are still in possession of the service provider, who may use this information for targeting strategies or even for manipulative scopes. From

[87] *Ibidem.*
[88] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *op. cit.,* 24-25.
[89] C. RIEFA, *op. cit.,* p. 4.
[90] B.B. DUIVENVOORDE, *op. cit.*, pp. 179 to 189.
[91] C. MACKENZIE, W. ROGERS, S. DODDS, *Vulnerability: New Essays in Ethics and Feminist Philosophy,* Oxford, Oxford University Press, 2014, pp. 8-9 mentioned by N. HELBERGER *et al., op. cit.,* p. 185.
[92] Art. 4 (4) GDPR.

the very moment in which the user employs the digital service, he becomes a potentially vulnerable person.[93]

- Systemic vulnerability

This persuasion profiling technique builds a true dependence of the customer to the digital service. This technique aims indeed to analyse user preferences to understand the choices that they are inclined to take and propose the most related content based on their interests. Persuasion profiling offers then the possibility for the digital service provider to release the best outcome. The more the user finds personalized content, the more he will keep using the same service. The more he uses this service, the more his behaviour will be studied. The more data are collected from a user, the more the service will improve (1) the suggestions and (2) the service choice architecture to give the customer the best experience. It is a cyclic, trustworthy and very asymmetrical relationship[94] between digital service recipient and digital service provider. In conclusion, the more insight the provider will have of a user, the more will be likely to find one's vulnerabilities and potentially exploit them. Vulnerability proportionally increases with the use of the service in question.[95] This process is called feedback loop[96], as already mentioned. Under this point of view vulnerability is systemic because it stems from the way a system shapes consumer behaviour. The legitimization for such mechanism is to be found in the setting of cookies or in the terms and condition that providers are obliged to propose: the problem, despite the conception of a "*an informed, observant and reasonably circumspect person*", resides in the consumers who do not read terms and conditions[97], neither refuse cookies. Afterall, it is quite fair when one looks at Microsoft terms and conditions, for instance, that would take almost an hour to be read by an average consumer, or by the choice to

[93] N. HELBERGER *et al.*, *op. cit.,* p. 185.
[94] *Ibidem,* p. 188.
[95] C. RIEFA, *op. cit.,* p. 15.
[96] *Ibidem.*
[97] *Ibidem,* p. 13.

refuse cookies which is sometimes inexistent.[98] This is more accentuated in vulnerable individuals.

Systemic vulnerability does not only stem from the structure of the market itself, but also from the structure of the regulatory system as a whole. Indeed, EU law is renowned for its *a posteriori* forms of redress[99], which must be initiated by the consumer, after having suffered from damage.[100] Lack or scarce of an efficient normative framework fails to assist consumers, thus contributing to render them more vulnerable. As descripted in Chapter 1, the average consumer standard suggests an active position of the consumer in the economic world: he must inform him/herself, critically observe and only then he/she could choose wisely. Consumers are on their own, once the trader provides them with a (prior) set of information.[101] Protection is constructed as a self-reliance mechanism.[102] If this model lacks realism in offline systems[103] (*see* Section on information overload), it lacks it even more in online systems.

So far vulnerability has proven to be situational, personal, temporary, constant, systemic, dispositional.

There are, in current researches fields, two conceptualizations of these categories: the class-based-approach and the state-based-approach.[104] The first one regroups the age, credulity and health conditions. The second one regroups all the other factors. If many critics have been addressed to the first category for over-stigmatizing groups of consumers[105] and ignoring all other sources of disadvantage, it is worth addressing a small critic also on the state-based approach, for ignoring the difficulty in acknowledging people who really need this particular protection. In this perspective, the next paragraph on intersectionality should help in shading some light on the question.

---

[98] It is not uncommon, in fact, to subordinate the access of a certain content to the consent of cookies. See in this regard C. RIEFA, *op. cit.,* p. 18.
[99] At least within Consumer law.
[100] C. RIEFA, *op. cit.,* p. 15.
[101] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *op. cit.,* p. 16.
[102] C. WILLETT, « Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive », *Journal of Consumer Policy,* 2010/33, p. 247.
[103] N. HELBERGER *et al.*, *op. cit.,* p. 196.
[104] N. MCSPEDDEN-BROWN, R. ODOKO, « Consumer vulnerability in the digital age », *OECD publishing*, n° 355, 2023, p. 5.
[105] N. HELBERGER *et al., op. cit.,* p. 178.

2.2. Intersectionality

Intersectionality is a theory that sheds light on the overlap in the same natural person of different factors and features that can be object of discrimination.[106] The purpose of the study was to prove that minority identities are affected by the system that leads them to greater oppression and discrimination, thus further marginalizing minority groups.[107]
The theory will help understand that multiple forms of disadvantages create obstacles that may be invisible to the conventional vision, thus unregulated.

A specific type of vulnerable person might be individually exposed to many needs and restraints (to a certain extent) while also encountering different forms of concurrent external factors of vulnerability. The ***ensemble*** of different types of vulnerabilities helps explain this overall loss of power, control[108] and agency together forming the main elements of the definition of vulnerability.

The innovation about this theory is indeed the consideration of all these factors as an ***ensemble***, rather than the consideration of each characteristic on its own. People who find themselves at the intersection between these factors could experience great discrimination on different levels and contexts.[109]

The fundamental ground of this theory on digital vulnerability is the following: disadvantages in the digital market are due to a combination of factors which influence each other. According to doctrinal categorization, the state-based approach regroups a set of (internal and external) interactive factors, of different duration (permanent or temporary).[110] In order to limit possible algorithmic discriminations, these factors should not be observed and treated as isolated elements, but as a whole. This is precisely what the theory of intersection has supported.
For instance, if examining closely the disadvantage that age may cause, it becomes clear

---

[106] Report of the Center for Intersectional Justice (CIJ) commissioned by the European Network Against Racism (ENAR), ***European Network Against Racism (ENAR),*** 2019, p. 7.
[107] ***Ibidem.***
[108] N. HELBERGER ***et al.***, ***op. cit.,*** p. 183: "*Thus, vulnerability is about one's relation to the world, the forces (social, physical, technical) in the world that can affect anything one deems important, and one's (lack of) control or power over those forces*."
[109] K.W. CRENSHAW, « Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics », ***University of Chicago Legal Forum***, 139, 1989, pp. 139-167.
[110] N. MCSPEDDEN-BROWN, R. ODOKO, ***op. cit***., p. 5.

that it is not age as such that renders or does not render someone weak. In case of elderly persons, for instance, is not the age that impairs them to take wise choices. It is, on the contrary, their limited digital capabilities, their loneliness or disability, together with their cognitive abilities.[111] It is a collection of factors that leads to a condition of disadvantage. The way that legal framework offers protection to them (which is information, source of *consensus*) leaves them without effective protection.

In fact, according to the European Commission's study on vulnerability, where it states that "*as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment*",[112] (*see* previous Section) a vulnerable people can encounter five different dimensions of vulnerability: at least a third out of more than ten thousand consumers show signs of vulnerability in multiple of these dimensions.[113]

A broader focus is therefore needed, because effective protection can only be achieved if addressing the intersection of the most relevant disadvantaging factors.[114] Hence, compared to vulnerability as conventionally conceived, intersectionality can be defined as a super plus vulnerability.

If potential biases in algorithms were treated as a whole, taking inspiration from this theory of intersectionality, the outcome would be entirely different. In fact, the vast majority of AI-based systems are structured so that all data are isolated: computing error rates pertain typically to single components, improving accuracy when computing different factors. The quality of the algorithm (the "algorithmic performance") lowers for intersectionality groups compared to persons associated only to one form of vulnerability.[115] Since the technical aspects of this matter are more complex than explained above, they fall within other fields of study (e.g. computer engineering), therefore this work will not give supplementary details beyond those previously provided.

---

[111] *Ibidem,* p. 18.
[112] Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union, *op. cit.,* p. 383
[113] Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union », *op. cit.*, p. 382.
[114] C. RIEFA, *op. cit.,* p. 16.
[115] A. HOWARD, « Real Talk: intersectionality and AI», available on https://sloanreview.mit.edu/article/real-talk-intersectionality-and-ai/ consulted on 01/08/2023.

What must be instead treated as a legal point of concern in this study is the result of this analysis, which is that appropriate protection can be only be achieved by taking into account all relevant sources of vulnerability and treat them as an interactive set of factors, including and influencing one another's. Vulnerable consumers are the norm and they should not be treated as an exception. However, adopting an "all-in" definition would create the exact opposite effect: incorporating all disadvantaged scenarios would not only be impossible but counterproductive. This is because if "vulnerable consumers" remains a substandard that applies to everyone, its effectiveness would then be jeopardized. Instead, this should become the new conception of consumers, thus admitting that also an average consumer can be vulnerable. A shift in paradigm is crucial: all consumers should be treated as vulnerable, thus expanding protection to them also. The point of depart should not be to provide less protection to some consumers while granting minimum and fictitious protection to others, all under guise of empowering even the most fragile. If individual characteristics such as stated in the UCPD are at the intersection with all the other characteristics, this would enlarge the basic protection. However, individuals who still remain more fragile than others due to intrinsic and permanent conditions, should be granted an even greater protection.

Moreover, this study suggests that gender can also produce vulnerability at the level of online B2C relationships.[116] For instance, in a 2015 study,[117] researchers have created fake Google accounts with the same settings and visited hundreds of employment webpages to let Google analytics know that they were looking for (the same) job opportunities. Ultimately Google showed 1852 times to male groups and only 318 times to female groups employment ads which promised higher salaries than the average[118], although both groups had visited the same pages and had the same profile settings. If gender equality in access to employment is a matter treated under other European fields of protection,[119] it does not exclude that digital vulnerability is a combination of factors that altogether provide a breeding ground for

[116] B.B. DUIVENVOORDE, *op. cit.*, pp. 189 to 191.
[117] A. DATTA, M. C. TSCHANTZ, A. DATTA, « Automated Experiments on Ad Privacy Settings. A Tale of Opacity, Choice, and Discrimination », *Proceedings on Privacy Enhancing Technologies,* 2015 (1), pp. 92 to 106.
[118] *Ibidem*, p. 93.
[119] See, for instance, the Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation.

exploitation.[120] This is in line with article 9 of the General Data Protection Regulation (GDPR), wherein gender, as a protected factor in the EU, cannot be processed unless explicit consent has been given.

[120] C. RIEFA, *op. cit.,* p. 12

Chapter 3

Legal framework

This chapter will analyse the current legal framework upon which vulnerable consumers may rely in the AI context. The instruments that will be studied are the following (in order of relevance): Unfair Commercial Practices Directive (UCPD), Proposal for a Regulation on Artificial Intelligence[121] (AI Act), Digital Service Act (DSA)[122], General Data Protection Regulation (GDPR).[123]

3.1 Unfair Commercial Practices Directive (UCPD)

The historical overview of the UCPD has already been presented in Chapter 1 of this work, hence this paragraph will be limited to analyse in detail what normative protection confers this instrument to the vulnerable.

Before all else, it is important to indicate that the scope of application *ratione materiae* of the Directive is very broad and includes any commercial practices and transaction, before – for instance with advertising – during and after their conclusion.[124] Its scope of application *ratione personae* includes any business-to-consumer transaction (B2C).[125] The UCPD does not exclude the application of other instruments regulating practices' fairness to consumers.[126] Reciprocally, the UCPD is

[121] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.
[122] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *O.J.,* L 277, 27 October 2022.
[123] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.,* L 119, 4 May 2016.
[124] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit.*, p. 5.
[125] Art. 3 (1) UCPD.
[126] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit.*, p. 9.

not excluded by the application of other instruments that may protect consumers against certain commercial practices. Article 5 works as a general provision of unfair practices, articles 6 and 7 deal with misleading practices while articles 8 and 9 deal with aggressive practices. Annex I contains a black list of commercial practices that are considered unfair in all circumstances.

Under the Directive, a commercial practice is unfair when it can alter the economic choices of a consumer group:[127] when the practice addresses a special category of consumers e.g. the vulnerable, the alteration must be addressed looking at the average member of that group.[128] If the response is positive, the practice could be defined as unfair thus prohibited. As being a Directive, it is not directly applicable to Member States[129] but it needs transposition into the domestic legislation of each State. Therefore, its rules on implementation are a matter of domestic law, in accordance with the principle of procedural autonomy.[130]

The potential alteration of consumers' behaviour is not the only condition to assess the unfairness of a practice. In fact, as evocated multiple times during this work, UCPD normative definition on vulnerability indicates only "*clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity*".[131] Through the Guidance written for the implementation of this Directive[132], it appears that the unfairness test related to age factor can be assessed by looking at different ages; in fact, there are certain practices that have greater potential to alter middle aged consumers (35 to 44 years old) than young consumers (16 to 24 years old) and *viceversa*.[133] The most vulnerable age category is children, due to their scarce experience and poor judgement skills.[134] That is why children derive protection stemming from both

[127] Art. 5 (2) b) UCPD.
[128] Art. 5 (3) UCPD.
[129] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *op. cit.,* p. 84.
[130] C.J.E.C., case *Courage and Crehan,* 20 September 2001, C-453/99, EU:C:2001:465, para. 29.
[131] *Ibidem.*
[132] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit.*
[133] Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union », *op. cit.*, sec. 2.6, p. 36.
[134] *Ibidem.*

article 5 (3) and from article n. 28 in Annex I, which entails the prohibition on direct exhortations, may it be aimed specifically at them or at adults with the intent of targeting children.

As for the category of credulity, the UCPD tends to englobe a vast number of consumers that for whatever reason, may be more susceptible than others to a certain practice. For instance, if a trader promotes the message that "for each purchased product, a tree will be planted" but has already committed to planting a precise number of trees regardless of the quantity of purchased goods, this will be considered unfair since it misleads consumers who are involved with environmental causes.[135] However, for any of these potentially unfair practices, the Court must evaluate a proportionality test : that will be considered as fulfilled only if a trader could have reasonably expected to alter the behaviour of a specific group.[136]

Transposed into online marketing practices, transactional decisions can be multiple and so can be their manifestations. For instance, someone's decision to continue using an online page is a transactional decision; its manifestation is the consumer that will continue to scroll through a feed.[137] As such, the UCPD can also be used to tackle systemic violation issues caused by the online choice structure (*see* Chapter 2) of the transactional decision of not switching to another good or service provider or to click on a surveillance advertising. The great power of the Directive results in not requiring to prove that the alteration of consumer's behaviour that has occurred *in casu*; it is enough to prove that the practice is "likely" to distort it. As it covers any transactional decision, the Directive will also protect any agreement to the processing of personal data i.e. the use of data for surveillance advertisings. The interface design, as well as its choice structure can be defined as a commercial practice thus under the scope of the UCPD. Annex I mention certain online practices that are

[135] *Ibidem,* p. 77.
[136] *Ibidem,* p. 36.
[137] The application of the UCPD to online practices has been confirmed in the Guidance on the Implementation of the Directive, under section 4.2.7. The UCPD also applies to practices that involve the use of AI, as confirmed by the Guidance under section 4.2.

irrefutably prohibited, e.g. "bait and switch"[138] practices and "nagging".[139] However, for RTB practices, the Directive does not insert a prohibition *per se*; on the contrary, it allows these practices as long as they inform the consumer about the dynamism of the price.[140] It does the same with price discrimination, that is applying different prices to different individuals for the same goods: this is not prohibited as long as the trader informs the consumer about the total price.[141]

As broad as the material scope of application of this Directive is and even if it tends to englobe online unfair practices, it does exclude any other source of disadvantage external to individual characteristics. The point of unfairness assessment is therefore restricted in relation to the multiple types of exploitative and misleading practices in the online market. Digital vulnerability is not entirely covered.

3.2 Proposal for a Regulation on Artificial Intelligence (AI Act)

Vulnerability currently stands as one of the main concerns in the creation of an AI legal framework, capable of conjugate both innovation and development of technologies, with the safeguarding of fundamental rights, laying an embankment to the risk of manipulation.

The AI Act is part of the digital Europe funding programme[142], designed to improve European competitiveness in the digital cross-border economy, eliminate fragmentation in digital legislation across the Union and strengthen European's capacities in key digital technology sectors. Preceded by several coordinated plans and

[138] Marketing technique aiming to attract consumers with an advertising on a certain good, then persuade them to buy a more expensive good. *See* p. 102, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit*.
[139] Practice consisting in repetitious behaviour to convince the consumer to consent to a request or purchase a good. *See* p. 102, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit*.
[140] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit*., p. 102.
[141] *Ibidem*.
[142] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, *O.J*., L 323, 19 December 2022.

Commission's communications[143], the prelude of the AI Act was the White Book on Artificial Intelligence[144], published in 2020. The intervention of the Parliament, the Council of the EU and the Commission have been multiple and this shows how essential was the creation of such legal framework. The expected path is to take the Union into a Digital Decade by 2030.[145] The Regulation was proposed in 2021 and aims at rendering AI trustworthy, so that every user can take advantage of what these technologies have to offer.[146]

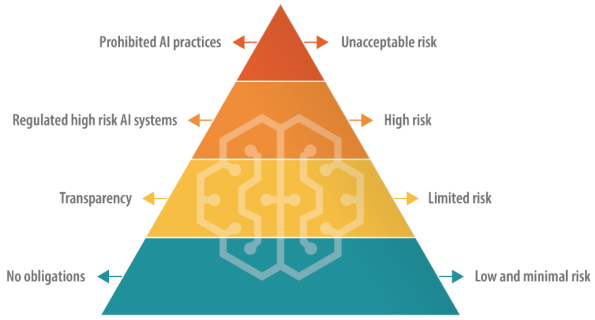
At the core of this instrument, the Commission puts its focus on the protection of fundamental rights[147], which is logical since the Union itself is entirely based on the idea of democracy, guaranteed by the respect of fundamental rights. The level of protection granted by this legislation appears to be minimal, as only minimum standards are regulated under the Proposal, leaving all the unregulated matters to the discretion of the Member States and the protection of the other relevant instruments depending on the circumstances of the case and its scope of application (e.g. GDPR requirements for the processing of data).[148]
The choice to regulate only the minimum necessary requirements seems to be justified by the urgency of a prompt action from the European institutions to legitimately counter-balance the increasing power of AI-based technologies towards the protection of users' fundamental rights.[149]

The underlying assumption under the structural choice of the AI Act may be that there is a difference between making one vulnerable and exploiting possible vulnerabilities.

---

143 For an exhaustive overview on the different instruments previous to the adoption of the Proposal for an AI Act: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence, consulted on 5/07/2023.
144 White Paper On Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 19 February 2020.
145 Art. 1 Decision […] establishing the Digital Decade Policy Programme 2030, *op. cit.*
146 Rec. 81 Draft AI Act.
147 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, « Artificial Intelligence for Europe », *op. cit.*, pp. 3, 14, 15.
148 Rec. 24 Draft AI Act.
149 Explanatory Memorandum of the European Commission of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, 2021/0106 (COD), sec. 2.4.

The entire Regulation consists in fact on a risk-based approach[150]: in its Title II, the Regulation lays down practices prohibited in all circumstances. In this point, the AI Act seems to reiterate the structure of the UCPD, which contains a black list of prohibited practices in all circumstances, which seems to be the same approach of Title II of this Regulation. The same act then proceeds, in its Title III, to list a classification of high-risk AI systems, which includes (1) those systems that are a safety component of a product (or a product itself) and that must undergo a third-party security assessment and (2) the AI systems contained in Annex III of the same Regulation. These types of AI systems are permitted but they must comply with a series of requirements listed in Chapter 2 of the same Title (risk management, operation's transparency, provision of information to users, human supervision, cybersecurity etc.). High risk systems are the object of 46 articles of the Regulation: the impact of this category could be so detrimental that the normative framework must assess complete rules to avoid such harmful effects. Also in this case, the categorization of high risk systems in Annex III appears to reiterate the UCPD "black-listing" structure. The classification then continues with the low AI systems risk, which require specific transparency obligations listed in Title IV, and minimal risk AI systems which are supposedly harmless for citizen and are, therefore, exempt from specific intervention, allowing a free use of such systems (e.g. videogames or AI-based spam filters). The risk-based approach structure results in a pyramidal organization of AI-systems.



Source: European Parliamentary Research Service, available on https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN

Figure 3.1: pyramidal structure of the AI Act

[150] Which would redirect to the idea of "making vulnerable": every AI-based software that would create a risk to natural persons should be regulated with different degrees of intensity. As for the exploitation of vulnerabilities, a special article is dedicated in the Regulation that will be subject of another paragraph in this work.

The AI Act includes of course all the subcategories of the artificial intelligence, hence ML is also covered, as suggested in article 3 (1) and explicitly mentioned in Annex I a).

It is important to highlight that the AI Act does not apply to private end-users; indeed, article 3 (4) excludes from personal scope of application the use of AI-systems in non-professional activities. End-users are not protected as such by the Regulation, but they are indirectly: the requirements weighing on providers aim to ensure that AI software respect the fundamental values of the Union, hence consumer protection.[151]

Reported below are all relevant provisions on vulnerability under the Regulation. This analysis is made comparing the initial proposal of the Commission with the proposed amendments of the Parliament.[152] This made clear (1) the legislative attempts to deploy further protection and (2) the institutions perspective in the matter.

- Recital 16

The first reference to vulnerable users that AI Act proposes is in its Recital 16. The importance of analysing the recitals is crucial, because recital are intended to justify the purpose of the act in its whole, meaning that this matter is being taken seriously by the legislative bodies of the Union. The initial formulation in the Proposal reads as follows:

> " *The placing on the market, putting into service or use of certain AI systems* ***intended to distort*** *human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. Such AI systems deploy subliminal components individuals cannot perceive or exploit* ***vulnerabilities of children and people due to their age, physical or mental incapacities.*** *They do so with the intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person. […] ".*

[151] Rec. 2 and 28 Draft AI Act.
[152] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, P9_TA(2023)0236 available on https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

After amendments of the EP, the recital currently reads as follows:

> " *The placing on the market, putting into service or use of certain AI systems* ***with the objective to or the effect of materially distorting human behaviour****, whereby physical or psychological harms are likely to occur, should be forbidden. […] Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of individuals* ***and specific groups of persons*** *due to* ***their known or predicted personality traits****, age, physical or mental incapacities,* ***social or economic situation****. They do so with the intention to or the effect of materially* ***distorting*** *the behaviour of a person and in a manner that causes or is likely to cause significant harm to that or another person* ***or groups of persons, including harms that may be accumulated over time****.* ***[…] it is not necessary for the provider or the deployer to have the intention to cause the significant harm, as long as such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices is complementary to the provisions contained in Directive 2005/29/EC, according to which unfair commercial practices are prohibited, irrespective of whether they carried out having recourse to AI systems or otherwise.****"*

This Recital explains article 5 (1) b) which states the same, using slightly different words that however leave the meaning unchanged.[153] The ultimate version of this recital includes a reference to manipulation: it underlines that, regardless of the intention of the provider, any practice that may cause an alteration of behaviour (because it was the objective of such practice or because it accidentally provides this effect *in ultimo*) is forbidden. This modification encloses an essential concern in the matter: for years the European Union has combatted for the elimination of the intent requirement when it comes to the establishment of a misleading practice. The UCPD effectively succeeded in this mission;[154] it would have been very unfortunate to go back to the *status quo* and reintroduce the intent requirement in this new legislation, as suggested in the initial formulation of the recital ("intended to distort"). However, article 5 (1) b) prescribes a

---

153 "*The following artificial intelligence practices shall be prohibited:* […] *(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a person or a specific group of persons, including characteristics of such person's or a such group's known or predicted personality traits or social or economic situation age, physical or mental ability with the objective or to the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is likely to cause that person or another person significant harm."*

154 N. HELBERGER *et al.*, *op. cit.,* p. 196.

causal link between the significant harm suffered by the vulnerable individual and the cause which must be the manipulative practice of the AI-system. The manipulative practice must be the ***conditio sine qua non*** for the harmful episode.[155] Since AI-system does not have a brain, it also does not have intentionality; however, the result of AI computation still remains detrimental. That is why the relevant factor is the outcome of the practice. Judges of national Courts in potential future caselaw will likely submit to the ECJ questions about the interpretation of the meaning of "significant harm". Optimistically this work anticipates that the meaning of significant harm will include not only physical harm, but also economic harm. It is indeed the position of the European Parliament, as referred to in the amendment for Recital 4.

The initial version of Recital 16 and its respective article 5 (1) b) almost reiterated ***mutatis mutandis*** the definition of vulnerability in article 5 (3) of the UCPD. In the current version, the definition has been broadened reaching now not only the intrinsic features of an individual, but also the social and economic context, may it be from explicit information given by the user to the provider ("known") or may it be from the presumed information extrapolated from data collection ("predicted").

The amended recital clearly refers to harm accumulated over time, which refers to multiple episodes of harmful practices, such as a specific pattern employed by the provider that will cause, over time and after repeated exposure to such pattern, a distortion in the behaviour of the vulnerable individual. This provision regulates possible systemic vulnerability.

The recital also rightly points out that the Regulation is only complementary to the UCPD, specifying that prohibited practices under the 2005 Directive remain forbidden, may they be conducted by human agents or AI agents.

- Recital 44

The AI Act fully recognizes the phenomenon of algorithmic discrimination. In its initial formulation, the recital reads as follows:

[155] If the practice would have not occurred, the harm would have not been the same.

> " *High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. […]* ".

Reported below the subsequent formulation of the same Recital:

> " *Access to data of high quality plays a vital role in providing structure and in ensuring the performance of many AI systems, […]. They should also have the appropriate statistical properties, including as regards the persons or groups of persons* ***in relation to whom*** *the high-risk AI system is intended to be used,* ***with specific attention to the mitigation of possible biases in the datasets, that might lead to risks to fundamental rights or discriminatory outcomes for the persons affected by the high-risk AI system. Biases can for example be inherent in underlying datasets, especially when historical data is being used, introduced by the developers of the algorithms, or generated when the systems are implemented in real world settings. Results provided by AI systems are influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable or ethnic groups, or racialised communities.*** *[…]* "

While in the initial formulation, the explanation about the rightness of the dataset is left out, in the final version it is further detailed that datasets can carry great biases which increase gradually with the employment of ML techniques (feedback loop). It specifies that these prejudices are particularly affecting vulnerable persons for reason of origin. It clearly addresses the concern over the perpetuation of biases prohibited under European legislation. The concern regarding predictive analytics, as explained in Chapter one, is evident and taken into consideration.

The key in the protection of vulnerability appears to be focused on high-risk systems only. In the latest amendments, a new Recital 58 a) has been added. It further develops how this category of AI-based systems can affect vulnerable **groups**, stating that "*the deployer should carry out a fundamental rights impact assessment prior to putting it* (the system) *into use. The impact assessment should be accompanied by a detailed plan describing the measures or tools that will help mitigating the risks to fundamental rights identified at the latest from the time of putting it into use*". However,

the same Recital further adds that "*This obligations should not apply to SMEs which, given the lack of resources, might find it difficult to perform such consultation*." The AI act consistently includes provisions exempting SMEs from the obligation that apply to providers of automated systems.[156] Therefore, a special protection is also granted to SMEs, as being equally perceived as vulnerable operators themselves in the digital market.[157] From an economic perspective, this seems justifiable by the objective of the digital package, which is the one of fostering industrial competitiveness. Nevertheless, this intention should not distract the European co-legislators from the very objective of the Regulation: enlarging recipient's protection, which strikes as being the case.

To complete this first section, a final analysis on article 7 (2) f) is important to be addressed. This article outlines the criteria that the Commission must consider when assessing whether an AI system poses a significant impact and risk to fundamental rights. The initial formulation reads as follows:

> " *The extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to* ***an imbalance of power****, knowledge, economic or social circumstances, or age;* "

The amended version, instead, reads as follows:

> " *The extent to which* ***there is an imbalance of power****, or the potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to* ***status****, authority, knowledge, economic or social circumstances, or age;* "

The acceptance of situational vulnerability becomes evident, thus it includes the position of the user in relation to the digital service provider (the "status") as a disadvantaging factor. This is by far the broadest normative definition of vulnerability[158] in the field; nevertheless, it applies only where AI systems might pose high risk to fundamental rights (and health and safety), thus severely restraining its use.

---

156 Rec. 72 and art. 55 Draft AI Act.
157 Explanatory Memorandum, *op. cit.,* sec. 1.1 and 3.3.
158 C. RIEFA, *op. cit.,* p. 11.

Another considerable accomplishment in terms of vulnerability may also be found in the type of control that the Proposal establishes: it requires, at least for high risk systems, an *ex-ante* control, which appears to – at least partially – redress the problem of systemic vulnerability, as addressed in Chapter 2, by transferring a part of the burden from the recipient (as an active actor who personally experiences harm) to the provider (as an active actor who must control the rightness of his activities).

The requirements deriving from categorizing a system at high risk are different.[159] For the purposes of this study, only the most relevant ones will be explained. Risk management is one of the first requirements listed in Chapter 2 of Title III; basically, it defines the obligation for the firms to priorly test their systems in order to verify their impact. The purpose is to put into the market the least harmful system. For the same purpose, datasets should be controlled in view of the elimination of possible biases and assessments on the relevant design choices, as prescribed in article 10 (2). In fact, the AI Act precisely formulates that datasets should be free of personal considerations, thus relying only on statistical properties of the individuals: the single datasets or their combinations as a whole must be unbiased.[160]

Most of the other requirements treat the transparency of the systems. Providers must inform the recipient about the intended purpose, circumstances that may lead to foreseeable risks and its performance with respect to the intended recipients of such system. The intervention of human oversight is thus not only strongly recommended but mandated. All these requirements are intended to minimise the potential risks in the mainframe of discriminative system, for instance. The underlying idea is the protection of users and indirectly of end users. The responsibility for the conformity relies upon providers, but the AI Act additionally prescribes coordination between manufacturers, importers and users aiming at informing inform the provider and national authorities of the non-compliance of such systems.

Whereas "*high-risk AI systems* (*that*) *have been trained and tested on data concerning the specific geographical, behavioural and functional setting within which they are intended to be used*",[161] a presumption of conformity is established. This means that in cases that

[159] Art. 9 to 15 Draft AI Act.
[160] Art. 10 (3) Draft AI Act.
[161] Art. 42 Draft AI Act.

the AI system produces a harmful impact on (vulnerable) people, the burden of proof relies on the victims to prove such damage and rebut the presumption. As inconvenient as this might appear from the victim's perspective, it is in line with the rationale of increasing industrial competitiveness, therefore avoiding excessive burden of responsibilities on providers. However, this Regulation does not create individual rights to people, thus the question of liability is not a regulated matter under the AI Act.

What arises from the Proposal is a clear concern on the negative impact that such systems could have. By exclusion, this pertains only for high-risk systems as having a greater potential to harm society: transparency and risk management are the two milestones that mitigate risk, while excluding – for the most – lower risks systems from these requirements. Vulnerability appears to be mentioned multiple times in the Regulation, as its exploitation is currently understood to be a concrete problem on the digital market: in relation to AI high risk systems, exploitation of vulnerabilities is a treated issue. Besides that, vulnerable people are considerably taken into consideration under the general prohibition of article 5 (1) b). However, the protection granted to the vulnerable under this general clause will be significantly different if the EP's amendments will not be adopted.

In fact it is important to underline that these amendments may also not be approved by the Council. The analysis above is indeed based upon the initial Commission proposal, followed by the amendments adopted by the European Parliament: this distinction has provided a comprehensive prospectus on the position of the institutions. If the Commission has a more outdated perspective on vulnerability[162], the Parliament has in contrast a more modern approach. Following the ordinary legislative procedure, the following phase is the first reading of the Council, which will decide whether to accept or refuse the Parliament's position; it would be very regrettable to depart from the

[162] Despite, however, having announced the necessity of a more dynamic vision of the concept.

modern outlook of the Parliament.[163] However, the majority of proposals are accepted during the first reading of the Council[164], therefore hope is pinned on that.

3.3 The Digital Service Act (DSA)

As previously stated, AI-based technologies can execute in a faster and superior way a range of tasks that were previously performed by humans.[165] In this perspective, it is appropriate to address a small number of considerations related to vulnerability under the Digital Service Act (DSA), which is a new instrument under European digital law whose purpose is to scale up digital services while reducing legal uncertainty for its providers and recipients.[166] It tackles societal risks caused by the new business models and services (e.g. online platforms). The scope of application *ratione personae* of the DSA covers services offered by intermediaries, hosting, online platforms and very large platforms offering services to recipients established in the Union.[167] The concern of the exploitative designs of platforms,[168] as well as surveillance advertisings[169] are in the scope of application of this Regulation. AI as a service (AIaaS), which is a new type of service wherein third-party providers offer "pre-customized" AI-empowering software to traders[170] is not explicitly caught into the scope of application but would seemingly fill in the definition of "provider" of article 3 DSA.

It is, also in the case of the DSA, a risk-based approach: if the service offered can put people in vulnerable situation, it must be forbidden or differently assessed in order to mitigate such risk.

---

163 In general, the Council always had a more progressive vision on vulnerability. Indeed, during the drafting for the proposal of amendments of the UCPD, the Council proposed a distinct standard of vulnerable consumers, independent to the one of the average consumer. This might suggest that the Council will adopt the AI Act Parliament's amendments.

164 https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview, consulted on 01/06/2023.

165 A. MONARCHA-MATLAK*, op. cit.,* p. 2079.

166 Art. 9 DSA.

167 Art. 2 (1) DSA.

168 Art. 25 DSA.

169 Art. 27 DSA.

170 European Commission, « AI-as-a-Service for the Deep Edge », DOI 10.3030/101015848, available on https://cordis.europa.eu/project/id/101015848/reporting

As for surveillance advertising, the DSA reflects to some extent a duty of fairness with respect to the self-assessment of risks: when offering a certain service to people in vulnerable situations, the provider should take measures to prevent, adjust or minimize potential biases.[171] The Regulation does not mention how providers should address this preventive analysis, nor it mentions how they should be aware that the recipient is in a vulnerable position. to further analyse the latter option, a distinction must be made between the content being entirely or mostly dedicated to them and the content that is indiscriminately accessible to all. If entirely addressed to minors, provider should take measures to increase their protection.[172] If not predominantly intended to underaged, the DSA does not explain how providers should assess vulnerability. In fact, according to Article 5 (1) c) of the GDPR, providers should not collect more data than required in order to assess the age of the recipient, nor they should collect this information prior to the employment of the service. Therefore, the Regulation does not provide further explanations on this matter. Moreover, it does not explain how the other vulnerable characteristics may be taken into account if they must conform to the principle of data minimisation of the GDPR.

At any rate, the DSA introduces in its article 26 (3) a ban on surveillance advertisings based on profiling using sensitive categories of data in the sense of article 9 (1) GDPR. It is undoubtedly one of the greatest achievements of the DSA in relation to vulnerability: the recognition of the immense power, influence and impact that such methods can have on the most vulnerable. However, the ban on targeting children and protected categories of persons does not apply to intermediary services and hosting services.[173]

The same applies to the concern around online choice structure, where the design of a website (and the underlying algorithm) is capable of rendering someone vulnerable. The Regulation lays down different provisions to regulate these exploitative techniques, mostly putting the focus on providing understandable information to the vulnerable or prohibiting design that impair the autonomy of the service recipients in general.[174] Article 25 instead prohibits the choice of a design that would manipulate

[171] Rec. 94 DSA.
[172] Rec. 89 DSA.
[173] Art. 19 DSA.
[174] Rec. 67 and art. 25 DSA.

recipients or alter their consent. Here vulnerability appears to be more widespread: a coherent and overall status of weakness applied to everyone. The same exception as that in the precedent paragraph is present in this instance: article 25 does not apply to intermediary services and hosting services.[175]

The DSA concentrates mostly on the protection of one special category of vulnerable: minors.[176] Several measures are taken to ensure their protection online.[177] As being part of a category of sensitive data[178], surveillance advertisings directed to minors – as already pointed out – are prohibited. Similarly to the protection of vulnerable people in the financial field, the DSA intends to complement the information requirements in case of minors with an additional element: comprehension. If a service is directed to underaged, the information must be presented as to be understandable by them.[179]

What remains notably blurry is precisely the definition of vulnerability. The DSA gives small directions on how to protect people in vulnerable situations, but does not mention, neither slightly, who are these persons. The question is approached from another focal perspective: situations that may render someone fragile. It is in line with the Regulation's structure, that is its risk-based approach. The only category explicitly mentioned is the one of minors[180], which is logical since one of the main purposes of this instrument is to increase minors' protection online.[181] As for the rest, it does not even redirect to another instrument in the field (e.g. the UCPD, which still remains the only instrument with a normative definition of vulnerability).

The "empowering through information" approach continues to exist[182] as an essential rule under the DSA, as explicated in its article 27. When a content provider uses an automated system, it shall advise about the parameters employed for the suggestion of content. The exception to intermediary and hosting service of system's transparency also exists in this case. However, article 27 prescribes that such

[175] Art. 19 DSA.
[176] Rec. 71, 81, 89.
[177] Art. 14 (3) and art. 28 DSA.
[178] Art. 9 (1) GDPR.
[179] Rec. 46 DSA.
[180] Recital 34 and Recital 68 DSA.
[181] Rec. 71 DSA.
[182] C. RIEFA, *op. cit.,* p. 16.

information must be included in the terms and conditions. Once again, a mere appearance of protection and transparency[183], since it has been shown[184] that terms and conditions – for being tremendously long and sometimes difficult to understand – are never read. Moreover, information in a general sense is not a useful tool for protection, even more so when there is excess of information excess, which can flawlessly be the case in the field of digital services. Information overload is currently at its apex.

If it is true that the DSA is a powerful instrument to regulate consumer protection regarding distance contracts, all the most important safeguards deemed to protect the vulnerable are only applicable to large and very large platforms. This leaves a potential detrimental gap.

3.4 General Data Protection Regulation (GDPR)

Since 2018[185], in the context of data, it is essential to talk about the General Data Protection Regulation (hereinafter, GDPR). This section will explain how the current legal framework can impede traders to make an abusive use of sensitive data.

The main purpose of this legal instrument is, as the name suggests, to give natural persons a high level of protection concerning the treatment of their personal data.[186] It is the first time in the history that the processing of personal data is recognized as a fundamental right. Moreover, whilst the GDPR does not admit the economic value of data as such, the Omnibus Directive assimilates the payment in currency with the one in data.[187] It is the strongest instrument in privacy and security law, not only within the European Union, but also outside, because its field of application applies to all

[183] K. POLUDNIAK-GIERZ, « Personalisation of Information Duties Challenges for Big Data Approach », *European Review of Private Law*, 2018/3, p. 298.
[184] C. RIEFA, *op. cit.,* p. 18.
[185] GDPR was approved in 2016 but entered into force in 2018.
[186] Rec. 1 GDPR.
[187] Indeed, the payment in data has been assimilated to the payment in currency with the Omnibus Directive that modified Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services.

companies, being them based the Union or not, for the simple reason of processing European data.[188] This is known as the extra-territorial effect of the Regulation.

The GDPR makes a clear distinction between sensitive and non-sensitive data. By exclusion, non-sensitive data are all the data that do not enter into the other category, which on the contrary includes all ethnic and racial origins, philosophical and political opinions, religion beliefs, sex life and sexual orientation, data related to health or genetics, trade union belonging and biometric data.[189] This special category calls for further protection compared to the non-sensitive data, as by nature they contain very delicate information related to someone's fundamental rights and freedoms.

This differentiation allows for the prohibition of automated profiling in the situation where traders acquire acknowledgement of vulnerable data which would be useful for targeting strategies. The technique would (un)fortunately falls under article 22 (4) of the GDPR, which means total prohibition, unless the automated profiling is used for purposes of public interest or if the user explicitly gives his consent. Consent to such practices is often distorted, though. With the advent of the GDPR, in fact, users must consent to the processing of data; so far, this is not surprising since the latest instruments in consumer policy give prominence not only to information but also to the willingness of giving free *consensus*, the latter becoming a predominant element in consumer protection. However, it is not uncommon for websites to unable access to their content without accepting cookies, for instance.[190] Users then become almost compelled to accept. The "free consent" could then be jeopardized. One must consider in fact that frequently information on automated profiling is to be found in the cookies pop-ups that systematically appear when entering a website.[191] If the provider is indeed obliged to advise the user about what will be done with his data once collected and refrain from deliver pre-ticked box[192], he should also be obliged to not mislead the user to push on the "accept" button rather than the "refuse" button. This practice is defined, together with others, "dark patterns" and currently falls under the scope of application of the

[188] Art. 3 GDPR.
[189] Art. 9 (1) GDPR.
[190] C. RIEFA, *op. cit.,* p. 18.
[191] F. MARTY, *op. cit.,* pp. 49 and 54.
[192] Rec. 32 GDPR.

UCPD as suggested by the Guidance of the Commission,[193] and also under article 25 DSA as having the effect to distort the recipients to make free decisions. Once again systemic vulnerability is currently regulated.

The special category of data lists inherent characteristics of the person, excluding all the characteristics that are beyond the simple ethnic origin or health conditions, which are predetermined personal features. Therefore, it does not prevent the absolute algorithmic discrimination. Hence, all other data that in combination with others may result in disadvantaging certain groups of consumers, are not taken into account. This is logical, since a far-reaching conception on sensitive data would have a disproportionate influence on traders. Additionally, the GDPR require from data controllers the adoption of preventive measures to limit discriminatory effects of data processing on individuals. However, as explained in Chapter 1, ML are inadvertently trained on biased datasets.[194] This specific case is thus out of the protection set in the GDPR.[195] Therefore, if GDPR enforces to give minimal – but essential – safeguards regarding certain data that may lead to discrimination when processed by AI-empowered systems, the solution on digital vulnerability cannot be found in this instrument.

To address some final words on the new digital framework, the notion of vulnerability as such is also excluded in other recent legislative modifications. The Digital Market Act (DMA), [196] whose purpose is fostering digital competitiveness and ensure consumers choices[197], does not mention vulnerable persons. It focuses on obligations of gatekeepers, prohibiting the impairment of consumers choices by unfair conducts.[198] For the rest, it redirects to the DSA and the UCPD.
Regrettably, also the current *Proposal on a Directive on the Liability for AI systems*

---

193 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit.*, p. 99.
194 F. ZUIDERVEEN BORGESIUS, *op. cit.,* p. 19.
195 C. ARGELICH-COMELLES, *op. cit.,* 10.
196 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *O.J.,* L 265/1, 12 October 2022.
197 Art. 1 DMA.
198 Rec. 4 and 37 DMA.

providers (the "AI liability Directive")[199] does not mention the vulnerable; it is the second expected instrument to complete the artificial intelligence framework. It will work, at least as reads the Commission's proposal, with rebuttable presumptions of causal link between the injuries caused by the system and the non-compliance of the latter with the AI Act obligations. This Directive should be helpful to (vulnerable) consumers, as it will apply between a user acting for personal activities and a user acting for professional activities.[200] Nevertheless, the path is long to its effective adoption and its possible application, since it has only been proposed in September 2022 and no common position from the Council has been adopted yet. Whilst its adoption, it should then be transposed into national legislation. This instrument would only contemplate a minimum degree of harmonization,[201] therefore letting the choice to regulate differently (only if granting higher standards) to the discretion of national legislators: a new and substantial fragmentation of digital legislation is to be expected.

On one hand, AI Liability Directive could grant individuals enforceable rights, on the other hand its application is not expected anytime soon[202]: in the interval, it is arguable that consumers could initiate proceedings under the UCPD or the current Product Liability Directive[203] if damages by certain AI systems are suffered, but vulnerable consumers would be left without any safeguard, as to those categories which do not meet intrinsic criteria set out in article 5 (3) UCDP. Not unexpectedly, compensation for occurrent damages will not be able to be repaired when the Directive will be transposed, for the notorious principle of non-retroactivity.

---

[199] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 28 September 2022, available on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496

[200] Art. 4 Draft AI Act.

[201] Rec. 14 Draft AI Liability Directive.

[202] Likely within two years from the adoption, as the deadline for transposing is generally of this duration.

[203] Efforts of reformation of this Directive have been made in order to adapt its interpretation to damages caused by AI systems. However, this leads to legal uncertainty because of the divergent interpretations that domestic Courts may give to a particular case.

3.5 Summary on the legal framework

To conclude this chapter, I endeavoured to create an explicative chart to provide clarity on the most relevant provisions addressing the issue of vulnerability.

Table 4.1: Current protection of vulnerable persons

Legal instrument	Relative articles	Protection beneficiaries	Substantive rules of protection (enforcement)
Unfair Commercial Practices Directive (UCPD)	Article 5 (3)	Clearly identifiable group of individuals who are vulnerable because of their personal characteristics (age, mental or physical health, credulity). Applicable only if the individuals are consumers.	Prohibition of practices that distort their economic behaviour, only by reference of the average member of the vulnerable group. Possibility to seek redress *ex post* to the national Courts according to domestic procedural rules.
Proposal for an Artificial Intelligence Act (AI Act)	Article 5 (1) b) (acc. to EP amendments)	Indirect protection: Individuals or group of individuals whose vulnerabilities are known or predicted, due to their personality traits, socio-economic situation, physical or mental health, age, credulity.	Prohibition of practices that cause significant harm to these individuals.
	Article 7 (2) f)	People in a vulnerable position *v-à-v* the provider due to an imbalance of power, their status, socio-economic situation, knowledge, age.	Categorization of this potentially dangerous AI-systems as high risk, from which derives reinforced obligations upon providers.

			Lack of redressing mechanism; the Regulation does not confer individual rights to people.
Digital Service Act (DSA)	Recital 62, 69, 94, 95, 104.	People in vulnerable situations, without further explanation of the concept. Minors are the only explicit category. No specific redirection in this regard to other legal instruments.	Possibility to only lodge an administrative complaint for the infringement of the Regulation. Lack of redressing mechanism; the Regulation does not confer individual rights to people.
General Data Protection Regulation (GDPR)	Article 9 (1)	Data related to particularly sensitive information that facilitate data-driven discrimination.	Administrative fines if non-compliance. Right to not be subject to automated decision-making (including profiling) if significantly affecting the individual.

Chapter 4

Final observations

4.1 From vulnerable consumer to vulnerable user

Chapter 1 exposed the origins of vulnerability within consumer policy. The concept was laid down for the first time in the UCPD, in its article 5 (3). Unfortunately, the normative definition is very restricted, and has not been reviewed in 2019 with the amendments enshrined in the Modernisation Directive.[204] In the previous sections the analysis has focused on current European Digital legislation in relation to vulnerable people. This analysis has not only been useful to affirm that a transformation took place within the modern legal framework, with the admission and the regulation – although in some cases – of a new conception of vulnerability. The analysis provided also a critical observation on a shift in paradigm: from vulnerable consumer to vulnerable user.

In fact, consumer protection appears to be in some way left out from the explicit concerns of the Union. In fact, although the Union explicitly admits that vulnerability is now also situational and relational in regard to latest digital developments[205], it does not change its normative definition with respect to consumers; yet it is only from a binding provision that derives the protection mechanisms. A consumer is a natural person who purchases goods and services for personal scope;[206] a user[207], instead, can be a natural or a legal person who uses an AI-system under its authority for a professional scope.[208] The *ratione personae* field of application of the AI Act does not cover consumers but it does indirectly since the impact of such AI systems is also experienced by consumers. Therefore, it

[204] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, *op. cit.*

[205] Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union. », *op. cit.,* p. 383.

[206] Art. 2 (a) UCPD.

[207] In the sense of the Proposal for an AI Act.

[208] Art. 3 (4) Draft AI Act.

appears logical to align the definition of vulnerability under Consumer law to the one proposed by the EP in article 5 (1) b) of the AI Act and not the contrary, as appears to be the Commission's standpoint.

This can be the reason why the AI Proposal worryingly does not mention consumers, besides when it (precisely) redirects to consumer protection regulatory framework[209] or when it comments that consumer protection is to be taken into account during the assessment of potentially high risk systems.[210] By all means, consumer protection is not an explicit objective under the Proposal. On account of its scope of application, AI Act operates with the same shared *ratio* as the funding programme that it belongs to, with the aim of bringing technology to businesses to enhance its application in wider and more reliable ways.[211] It only marginally treats consumers, redirecting *quasi* systematically this question to more specific instruments such as the UCPD. With the AI Act, the distinction between consumer and user has been made very clear. Consumer protection is part of the latest regulatory framework as an element to be considered within fundamental rights respect, but it is regulated in different instruments, which are more specific and apparently more exhaustive.

Vulnerability under consumer law is thus completely different from vulnerability under digital law. Although the first should receive equal protection as the one granted to users, and be abreast of the most recent digital development, the co-legislators seem to ignore this concern and treat these two categories (consumers and users) as diametrically opposite, except when it is somehow referring to the concept of digital vulnerability contained in the UCPD.

If the underlying premise of the latest instruments is that "what is illegal offline should be illegal online"[212], it would be more consistent to align the UCPD to the digital reality. Vulnerability under digital law is conceived in relation to the risks that a system can cause to an individual: the more dangerous is a system, the more it will

[209] Explanatory Memorandum, *op. cit.,* section 5.2.2 (p. 13).
[210] Rec. 28, Draft AI Act.
[211] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, *op. cit.*
[212] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « Tackling Illegal Content Online Towards an enhanced responsibility of online platforms », *Publications Office,* COM(2017) 555 final, 28 September 2017.

put the recipient in a disadvantaging position. Relational vulnerability is not only admitted, but most importantly regulated.

Furthermore, the role of consumer itself has changed: consumers have a more crucial position in changing market's economy than before. They have currently become real-time active actors, for instance with Real Time Bedding techniques (RTB). They think to see what the trader wants to offer them or to pay for an established price, but in reality they are seeing what the trader thinks that they would like to see and pay how they are likely willing to pay (WTP).[213]
This justifies the birth of a new actor in the digital era: the prosumer.[214] This concept defines a natural person who is both a professional and a consumer.

Because of the latest digital market developments, the unequal position that consumers experience is deeper; the position of traders is, at this point, at its strongest advantage. The alignment of the oldest notion to the newest should reduce the fragmentation of the regulative frameworks in the digital sector, which is precisely one of the objectives affirmed in the Digital EU strategy.[215] Moreover, it would concretely empower consumer protection which is part of another EU strategy[216] and a fundamental value of the Union. This would clearly avert the legislator from his esteemed average consumer standard, irrevocably admitting that this benchmark has now become obsolete.[217] A proof of humbleness and pride to abandon this standard, which was undoubtedly a great jurisprudential construction when the market was predominantly offline.

Abandoning the idea of the "average" and its subsequent substandard "vulnerable" is not unconceivable: the ECJ has already extended the condition of vulnerability in

---

[213] F. MARTY, *op. cit.,* pp. 52, 53 and 70.
[214] G. BELTRA, « The consumer-policy nuts and bolts of the sharing economy », *BEUC,* 2016, available on https://www.beuc.eu/blog/the-consumer-policy-nuts-and-bolts-of-the-sharing-economy/
[215] Briefing of the European Parliamentary Research Service, PE 733.519, 2023, available on https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733519/EPRS_BRI(2022)733519_EN.pdf. See also: Rec. 4 DSA, Rec. 2 Draft AI Act, Rec. 9 DMA.
[216] Communication from the Commission, « New Consumer Agenda, Strengthening consumer resilience for sustainable recovery », *O.J.,* COM (2020) 696 final, 13 November 2020.
[217] G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *op. cit.,* p. 3.

relation to the conclusion of online contracts to all consumers.[218] Here, vulnerability is assessed in light of external factors, where any individual can be misled, independently of his age or health condition.

The current consumer policy needs a clear dichotomy between the vulnerable and the more vulnerable, as clearly pointed out from the consumers themselves in the 2022 public survey of the Commission.[219] All consumers should be considered as vulnerable to some extent, because of the multiple marketing strategies and structures that pose them at disadvantage. The role that vulnerability plays must change: it must not be considered as exceptional but rather as the minimum standard applicable to all consumers. This is more accentuated when interacting with AI systems, that are able to consider hundreds of variables, in different combination, all possibly leading to discrimination.

There is a failure in the system in recognizing and addressing the specific needs of the vulnerable because of the inadequacy of its conception (systemic vulnerability). The current conception within consumer policy privileges some characteristics of vulnerability (the intrinsic) to the detriment of all the others. They are considered unequally. In the current consumer law, there is a lack in the overall consistency between different conception of vulnerabilities (in the UCPD, in the AI Act, in the other instruments that – for coherence's sake – this work only mentioned in the footnotes).

More guarantees to the vulnerable are expected if granted uniformly and equally. If the co-legislators seem to reserve different conceptions of vulnerability according to the type of service that the individual is confronting[220], this does not, in any case, justify the lack in making clear any others considering criteria that may trigger this special protection beside the one listed in article 5 (3).

---

[218] C.J., GC, case *Pammer and hotel Alpenhofp,* 7 December 2010, joined cases C-585/08 and C-144/09, EU:C:2010:740, para. 59 and 62: "*with regard to new means of communication and the development of electronic commerce* […] *which makes it more difficult to determine the place where the steps necessary for the conclusion of the contract are taken and at the same time increases the vulnerability of consumers with regard to traders' offers*."

[219] Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union », *op. cit.*

[220] For instance, in the AI Act vulnerability is assessed with regards to the possible risk that the system could provoke to the individual.

4.2 Proposed solutions

Before entering into details, it is necessary to establish the following preliminary statement: the proposed solutions acknowledge that its unfeasible to define the algorithm's inputs target variables to wholly eliminate discrimination. This is because, target variables themselves stem from competing definitions of disadvantaging factors and result in an incommensurable combination of those. This work concentrates its solutions on *ex post* forms of protection, in line with the consumer policy in the matter and taking into account that more technical solutions regarding AI functioning are out of the scope of this study. Starting from this assumption, the following resolutions are suggested.

4.2.1 Undermine information empowering

Foremost, information should not be the main vehicle of protection, despite the current regulatory framework in the matter, but also the one suggested under the New Consumer Agenda.[221] Information overload increases with GDPR and the new DSA, that impose additional information requirements. The informational model in the digital market, which promotes the concept of informed consent, offers in reality a mere appearance of protection[222], precisely because of its excess. Information overload creates a digital asymmetry which cannot be tackled by providing other information requirements. Consenting becomes sometimes a constraint, a fictitious thought.

If information empowering cannot be eradicated in the absolute[223], some marginalizing measures should at least be taken into account to allow deep understanding of such information to consumers, for instance completing article 14 (5) DSA related to providing a summary of the terms and conditions key words. It

[221] Communication from the Commission, « New Consumer Agenda, Strengthening consumer resilience for sustainable recovery », *O.J.,* COM (2020) 696 final, 13 November 2020.
[222] K. POLUDNIAK-GIERZ, *op. cit.*, p. 298.
[223] C. RIEFA, *op. cit.*, p. 22.

should be added that such summary should appear in the first page, perhaps indicated in bold writing.

Additionally, this work does not intent to ignore the co-legislator's rationale of avoiding an excessive burden of obligations on traders; it would discourage online transactions and reduce the fostering of digital market, which remains the main objective of all the treated legislations of this study.[224] If it is true that this work argued for a universal and global approach to vulnerability, it does not ignore the fact that remedies may be triggered only when the breach has occurred *in casu*. Enlarging vulnerability protection to situations of all kinds would mean to render the protection evanescent, thus useless and ineffective.

4.2.2 Digital vulnerability standard

For an up to date and effective enforcement of the Directive, article 5 (3) UCPD should be modified to include other characteristics of vulnerability and their respective combination that could lead to an excessive imbalance of power. It is important to introduce a stand-alone standard in the UCPD: the "digital vulnerability benchmark", its relevancy submitted to the only condition of operating with consumers on online marketplaces.

Article 5 (3) could thus be redacted as follows:

> "*3. Commercial **online** practices which are likely to materially distort the economic behaviour of consumers who are particularly vulnerable to the practice or the underlying product because of an **excessive imbalance of power or because of socio-economic factors**, mental or physical infirmity, age, credulity, in a way which the trader could reasonably be expected to foresee. This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or statements which are not meant to be taken literally.*"

[224] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *op. cit.*: "*UCPD is based on the idea that, for instance, a national measure prohibiting claims that might deceive only a very credulous, naive or cursory consumer (e.g. 'puffery') would be disproportionate and create an unjustified barrier to trade*."

When confronting a consumer on the digital market, the standard to assess whether a certain practice is misleading or not, should be in light of a broader conception than the customary one. With the introduction of a clear benchmark as a stand-alone standard, this would both enlarge and delimitate the scope of application of article 5 (3). This would allow the domestic Courts to be sure of granting a useful protection to the right persons. It is not impossible to conceive within consumers policy different levels of vulnerability, since for instance a category of "vulnerable" and a category of "very vulnerable" people have been recognized in the *Guidelines for the management of the European Union Rapid Information System* (the ancient RAPEX – today called Safety Gate), which is a powerful alert system for dangerous products in the existing consumer policy.[225]

A neglected aspect of introducing a normative definition of this stand-alone principle of digital vulnerability is its effect in domestic procedures. Indeed, procedural rules implementing the rights established for the benefit of consumers are a matter of national law where the Union gives the member States national procedural autonomy.[226]

The ECJ has made clear in numerous judgments that the national courts must raise of their own motion the exceptions drawn from the European consumers directives.[227] The matter of the mandatory nature of the directive's transposed provisions and the possible waiver by the consumer is therefore a matter of domestic law. The *ratio legis* of consumers legislation is usually decisive in favour of the judge raising by their own motion; the objective of protection sought by the European legislator would not operate if the application of the provisions were subordinated to their invocation by the beneficiary.

Moreover, if this assessment was left to the discretion of the national courts, the criteria on which they would base their *ex officio* actions in some cases and not in

[225] Respectively: children from 8 to 14 years old, persons with reduced cognitive capabilities or knowledge and very young children, persons with extensive disabilities.

[226] C.J.E.C., case *Océano Grupo,* 27 June 2000, C-240/98, EU:C:2000:346, point 26 and C.J.E.C.., case *Mostaza Claro,* 26 October 2006, C-168/05, EU:C:2006:675, point 38.

[227] C.J., case *Banco Español de Crédito*, 14 June 2012, C-618/10, EU:C:2012:349, para. 41 to 43 and C.J., case *Aziz,* 14 March 2013, EU:C:2013:164, C-415/11, para. 46.

others would not be clear, leaving the place for legal uncertainty.[228] The introduction of a normative definition of the principle would definitely allow greater protection and would narrow regulatory uncertainty.

As inconvenient this may appear, it is however very much appropriate to reserve a broader definition of vulnerability only in specific cases (emphasizing on the one proposed by the Parliament with regard to high-risk systems). An "all-in" definition would rather create the opposite effect, hence discrediting the powerfulness of an increased protection, granting safeguards also to individuals who do not need it. This is the reason why this new standard should only apply in online transactions.[229]

4.2.3 UCPD to tackle intersectional vulnerability

Moreover, the UCPD could clarify in its article 5 (3) that the intersection of different axes of vulnerability (intersectionality) should be considered when assessing if a practice altered the behaviour of the vulnerable, therefore eliminating any doubt that (1) such situation exists and (2) concerning which exact factors may or not have led to the specific circumstances of the case.

4.2.4 Prohibition on surveillance advertisings

In harmony with the duty of diligence, it could be convenient to introduce a prohibition on surveillance advertising.

Alternatively, it would be preferable to introduce an obligation on traders to set contextual advertisings by default, unless the recipient takes deliberate action to switch to surveillance advertisings. Contrary to the current approach of the DSA, which allows surveillance advertising on the condition that the recipient is being informed

---

[228] A. JEAUNEAU, *L'ordre public en droit national et en droit de l'Union européenne : essai de systématisation,* Paris I, Hal, 2015.

[229] In this respect, this conception differs from the global conception as suggested by Helberger, who in the contrary intends to create a global conception *"to capture all those ways in which consumers can be affected adversely by actors in digital marketplaces without being able to prevent those occurrences." (*N. HELBERGER *et al.*, *op. cit.,* p. 183.)

about the parameters employed in the ad[230], and several other information requirements to display in the same advertising, this work suggests a prohibition on surveillance advertisings, in agreement with the one towards minors of article 24 b) DSA. This provision should be applicable to all service providers, without the exception on intermediary and hosting services.

Following the structure of the DSA, it should then be added in the first section, ideally after article 15. Alternatively, it could be introduced as a point 4 in article 26, specifically addressing that is applicable to all intermediary services.

4.2.5 Enforcement mechanisms

Furthermore, as regarding the AI Act, it would be more appropriate to foresee judicial enforcement mechanisms in the Regulation itself. The Act does not confer individual rights to individuals: this means that (vulnerable) consumers are left harmless if suffering damages from an AI-based system. As already pointed out, the AI liability Directive should be the instrument granting *ex post* mechanisms of redress to natural persons but its adoption is not expected soon.

With the same underlying idea, the DSA should add to the possibility of lodging an administrative claim,[231] a provision granting individuals an enforceable right to seek redress in case of suffered harm. The same considerations of the previous paragraph are arguable here.

4.3 Subsidiary remarks

Lastly, as mentioned in the previous section, abandoning the idea of the average consumer as a powerful and attentive person, should also meet the international doctrine on vulnerability. For instance, the International Organization for

[230] Art. 26 DSA.
[231] Art. 53 DSA.

Standardization (ISO)[232] explicitly affirms, in its guidelines, that assessing the fairness of practices upon the needs of the average consumer is detrimental for everyone, especially to the vulnerable. The question remains open as whether the Union will likely decide to conform to such advice.

The judicial must play a great role: judges will have to ensure, for example, that the general ban on exploiting vulnerabilities of AI systems is interpreted very strictly with regard to minors, guaranteeing the application of the prohibition and its relative burden of proof will be assessed considering their age and needs.

As for the rest, as all self-respecting change, the burden is shared between the regulatory power, on which relies the initiative itself, the companies that should respond to this concern, for instance, with periodical surveys or reports, and society as a whole, on which depends the education towards inclusivity, for instance with campaigns and private projects.

[232] "*Overly standardized services designed to meet the needs of the "average consumer" can be detrimental and even cause harm where consumers in vulnerable situations are negatively impacted. Services need to be designed with sufficient flexibility to support changes in consumer circumstances and staff should be empowered to provide tailored solutions to consumers."* Available on https://www.iso.org/contents/news/2022/05/looking-out-for-vulnerable-consu.html

Conclusion

Through this study it was possible to identify the evolution of vulnerability and its implications with regard to AI-based technologies and its risks, to analyse its legal implications and the fields wherein a stronger intervention by the co-legislators is required.

The main consideration that arises from this study is that the notion of vulnerability differs in its application with respect to different fields of action of the Union. The concept has a polysemic use that reflects the heterogeneity of the risks in these different fields. With the recent publication of the UCPD Guidance, efforts have been done in order to broad this notion within European consumer law in view of the exploitative market practices that took the leadership in the last years. Almost simultaneously, the necessity of the adoption of a framework to regulate new AI technologies urged to be adopted. With the AI Act as proposed by the Commission, vulnerabilities seem to reiterate the outdated conception of the UCPD; on the contrary, the AI Act as proposed with the EP amendments, gives a wider perspective on vulnerabilities thus enlarging its consequent protection.

May the Council adopt or reject the Parliament's amendments, the AI Act could strengthen its efficacity by introducing redress mechanisms in it. As for the other instruments on which vulnerable consumers may rely to seek redress, the UCPD would need the introduction of a normative definition of digital vulnerability, therefore creating a new and independent standard from the average consumer benchmark. Indeed on the online market the average consumer cannot be as attentive and circumspect as when the market was predominantly offline, due to incommensurable information overload. In digital transactions, every individual may be vulnerable to some extent. The Union would need to abandon the average to contemplate overall vulnerability.

Protecting the vulnerable is, eventually, protecting everybody.

Bibliography

Legislation

Art. 169 TFEU.

Art. 12 TFEU.

Art. 4 (2) TFEU.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, *O.J.,* L 149/22, 11 June 2005.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, *O.J.*, L 304, 22 November 2011.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.,* L 119, 4 May 2016.

Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, *O.J.,* L 328/7, 18 December 2019.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *O.J.,* L 265/1, 12 October 2022.

Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 28 September 2022, available on https://eur-lex.europa/eu/legal-content/EN/TXT/?uri-CELEX%3A52022PC0496.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *O.J.,* L 277, 27 October 2022.

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, O.J.., L 323, 19 December 2022.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « Tackling Illegal Content Online Towards an enhanced responsibility of online platforms », ***Publications Office***, COM(2017) 555 final, 28 September 2017.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, « Artificial Intelligence for Europe », COM (2018), 237 final, 25 April 2018.

White Paper On Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 19 February 2020.

Communication from the Commission, « New Consumer Agenda, Strengthening consumer resilience for sustainable recovery », *O.J.*, COM (2020) 696 final, 13 November 2020.

Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *O.J.*, C 526/1, 29 December 2021, p. 99

Explanatory Memorandum of the European Commission of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, 2021/0106 (COD), sec. 2.4.

Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, P9_TA(2023)0236 available on https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.

Report of the European Commission on Consumer Vulnerability across Key Markets in the European Union, *Publications Office*, 2016, p. 5.

Study for the Fitness Check of EU consumer and marketing Law - Final report Part 1 - Main report, European Commission, DS-02-17-420, 2017.

Briefing of the European Parliamentary Research Service, PE 733.519, 2023, available on https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733519/EPRS_BRI(2022)733519_EN.pdf

Case Law

C.J.E.C., case *Cassis de Dijon*, 20 February 1979, C-120/78, EU:C:1979:42, para. 13.

C.J.E.C., case *Gut Springerheide*, 16 July 1998, C-210/96, EU:C:1998:369, para. 31.

C.J.E.C., case *Océano Grupo*, 27 June 2000, C-240/98, EU:C:2000:346, point 26

C.J.E.C., case *Corsten*, 3 October 2000, C-58/98, EU:C:2000:527, para. 38.

C.J.E.C., case *Courage and Crehan,* 20 September 2001, C-453/99, EU:C:2001:465, para. 29.

C.J.E.C., case *Mostaza Claro*, 26 October 2006, C-168/05, EU:C:2006:675, point 38.

ECJ., GC, case *Pammer and hotel Alpenhofp*, 7 December 2010, joined cases C-585/08 and C-144/09, EU:C:2010:740, para. 59 and 62.

ECJ., case *Banco Español de Crédito*, 14 June 2012, C-618/10, EU:C:2012:349, para. 41 to 43.

ECJ., case *Aziz,* 14 March 2013, EU:C:2013:164, C-415/11, para. 46.

C.J., case *Kásler*, 30 April 2014, C-26/13, EU:C:2014:282, para. 60.

Legal doctrine

ARGELICH-COMELLES, C., *Inteligencia Artificial y tratamiento legal de la discriminación algorítmica en los online marketplaces de consumo*, thesis, Universidad Autónoma de Madrid, 2022, pp. 7 to 10.

BELTRA, G., « The consumer-policy nuts and bolts of the sharing economy », ***BEUC***, 2016, available on https://www.beuc.eu/blog/the-consumer-policy-nuts-and-bolts-of-the-sharing-economy/

CRENSHAW, K.W., « Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics », *University of Chicago Legal Forum*, 139, 1989, pp. 139 to 167.

DATTA, A., TSCHANTZ, M.C., DATTA, A., « Automated Experiments on Ad Privacy Settings. A Tale of Opacity, Choice, and Discrimination », Proceedings on Privacy Enhancing Technologies, 2015 (1), pp. 92 to 106.

DUIVENVOORDE, B.B., *The consumer benchmarks in the Unfair Commercial Practices Directive*, Amsterdam, Springer*,* vol. 5, 2015, pp. 13 to 27, pp. 179 to 191.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, « BigData: discrimination in data-supported decision making », 2018, p. 13, available at https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, « Bias in Algorithms – Artificial Intelligence and Discrimination », *Publications Office*, 2022, pp. 8-9.

GOFFAUX, B., « Le devoir général d'information dans le droit belge de la consommation », *D.C.C.R.*, 2013, pp. 253 et seq.

GRAY, H.M, GRAY, K., WEGNER, D.M., « Dimensions of mind perception », Science, 315(5812), 2007, p. 619.

HELBERGER, N. *et al.,* « Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability », Journal of Consumer Policy, 175-200, 2022, pp. 177 to 196.

HILL, R.P., SHARMA, E., « Consumer vulnerability », *Journal of Consumer Psychology,* 30/3, pp. 551 to 570.

HOWELLS, G., TWIGG-FLESNER, C., WILHELMSSON, T., *Rethinking EU consumer law*, Routledge, New York, 2018, pp. 3 to 106.

JEAUNEAU, A., *L'ordre public en droit national et en droit de l'Union européenne : essai de systématisation*, Paris I, Hal, 2015.

KODIYAN, A. A., « An overview of ethical issues in using AI systems in hiring with a case study of Amazon's AI based hiring tool », *Researchgate Preprint*, 2019, pp. 1-2.

MACKENZIE, C., ROGERS, W., DODDS, S., *Vulnerability: New Essays in Ethics and Feminist Philosophy,* Oxford, Oxford University Press, 2014, pp. 8-9.

MARTY, F., « Plateformes numériques, algorithmes et discrimination », *Revue de l'OFCE*, 2019/4 164, pp. 48 to 70.

MCSPEDDEN-BROWN, N., ODOKO, R., « Consumer vulnerability in the digital age », *OECD publishing*, n° 355, 2023, p. 5.

MONARCHA-MATLAK, A., « Automated decision-making in public administration », *Elsevier B.V,* 192/2021, pp. 2078-2079.

PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY, « The impact of the General Data Protection Regulation (GDPR) on artificial intelligence », *European Parliamentary Research Service*, PE 641.530, 2020, p. 15.

PITARDI, V. *et al.,* « Service Robots, Agency, and Embarrassing Service Encounters », Journal of Service Management, vol. 33/2, 2022, pp. 389 to 414.

POLUDNIAK-GIERZ, K., « Personalisation of Information Duties Challenges for Big Data Approach », European Review of Private Law, 2018/3, pp. 298.

RIEFA, C., « Protecting vulnerable consumers in the digital single market », *European Business Law Review,* 2022, pp. 4 to 22.

SICILIANI, P., RIEFA, C., GAMPER, H., *Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement*, Oxford, Hart Publishing, p. 18, partially available on Google Scholar.

SUNNY TSAI, W-H. *et al*., « Human versus chatbot: Understanding the role of emotion in health marketing communication for vaccines », Wiley, 2021, vol. 38/12, , pp. 2378 to 2381.

WIEWIOROWSKA-DOMAGALSKA, A., « Contribution to growth. Legal Aspects of Protecting European Consumers, Study for the Committee on the Internal Market and Consumer Protection », Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 79.

WILLETT, C., « Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive », *Journal of Consumer Policy,* 2010/33, p. 247.

ZUIDERVEEN BORGESIUS, F., *Discrimination, artificial intelligence and algorithmic decision-making*, Strasbourg, Directorate General of Democracy, 2018, pp. 12 to 22.

Other

14th annual report of the Future Today Institute on Strategic trends that will influence business, government, education, media and society in the coming year, 2021, p. 8, available on https://www.pta.es/wp-content/uploads/2022/12/FTI_2021_Tech_Trends_Volume_1_AI.pdf

13th annual report of the Future Today Institute on Strategic trends that will influence business, government, education, media and society in the coming year, 2020, p. 27, available on https://www/shannonweb.net/wp-content/uploads/2020/06/FTI-2020-Trends-Report.pdf

Room Document of the European Data Protection Supervisor (EDPS) for the 38th International Conference of Data Protection and Privacy Commissioners, 2016, p. 4, available at https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en

Report of the Center for Intersectional Justice (CIJ) commissioned by the European Network Against Racism (ENAR), *European Network Against Racism (ENAR),* 2019, p. 7.

HOWARD, A., « Real Talk: intersectionality and AI» , available on https://sloanreview.mit.edu/article/real-talk-intersectionality-and-ai/

European Parliament
https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview

CORDIS European Commission
European Commission, « AI-as-a-Service for the Deep Edge », DOI 10.3030/101015848, available on https://cordis.europa.eu/project/id/101015848/reporting

International Organization for Standardization
https://www.iso.org/contents/news/2022/05/looking-out-for-vulnerable-consu.html

Acknowledgements

I would like to sincerely thank my supervisor, Professor Francq, and my co-supervisor, Professor Fallon, for their time, attention and invaluable insights.

My deepest gratitude extends to my family. To my mother, the strongest woman I now, for always being so supportive. I wish to dedicate all my achievements to you.
To Marco, for encouraging me from my earliest years to learn, to study, to focus, to dedicate. Thank you for teaching me the meticulousness in doing things and seeing the world.
To Alessia, for being my daily inspiration. Your constant support, understanding, and motivation are my driving force. Thank you for being my safe harbour.
To Thomas, for having placed great trust in me since the beginning. You warmly welcomed me during the peak of my teenage years and for that, I am profoundly grateful.
I owe specific thanks to Samuel, for enlightening all my days. You are now too young to understand these words, but I hope one day you will read these lines and feel the endless love I have for you. I will stand by your side through all the achievements you will accomplish, supporting you in every step of your life, exactly how your mother did with me.

I also wish to thank my long-distance friends for holding my hand tightly over these years. "*There's no such place as far away. Can miles truly separate you from friends?*"
To Fao, for always being such a good friend. So understanding, spontaneous, and sincere.
To Elettra, the friend soulmate that I did not know I had.

To my Belgian friends, for welcoming me when I could scarcely string three words together in French. You have all taught me a lot during these years and helped me believe that I belong here.

I am truly grateful to every person who has stood by me throughout these years; you have all given me the strength to carry on. I feel so lucky to have you all in my life.
I also want to thank those who were once part of my life but somehow are no longer; you have contributed to my resilience and growth.

Lastly, I acknowledge myself. Through determination and unwavering resolve, I always found the strength to persevere. It takes courage, after all, to never look back but always forward.

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**