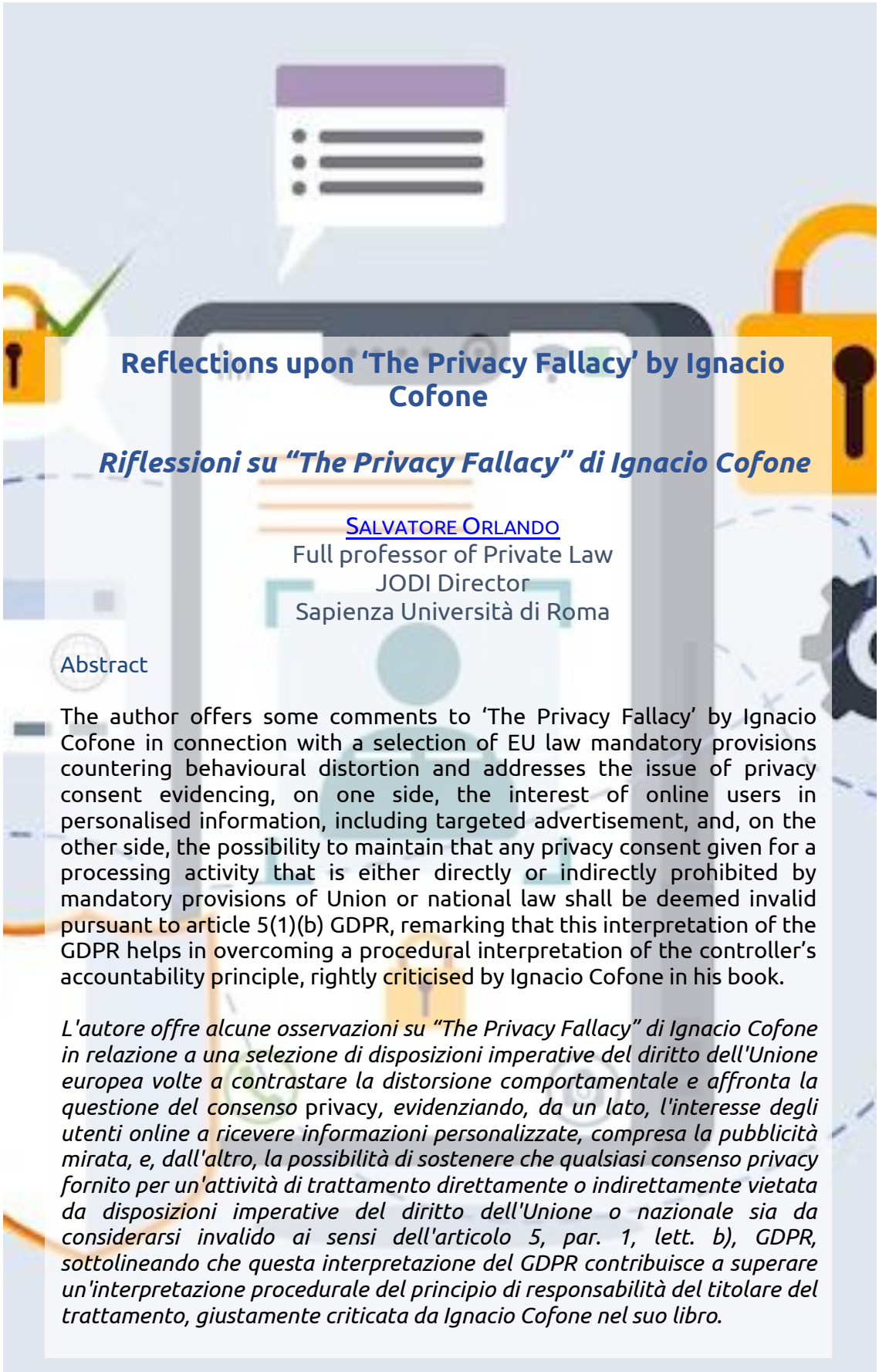
Orlando S, 'Reflections upon 'The Privacy Fallacy' by Ignacio Cofone' (2025) Special Issue 1 EJPLT.
DOI: https://doi.org/10.57230/EJPLTSI251SO

EJPLT
ISSN 2704-8012



Reflections upon 'The Privacy Fallacy' by Ignacio Cofone

Riflessioni su "The Privacy Fallacy" di Ignacio Cofone

SALVATORE ORLANDO
Full professor of Private Law
JODI Director
Sapienza Università di Roma

Abstract

The author offers some comments to 'The Privacy Fallacy' by Ignacio Cofone in connection with a selection of EU law mandatory provisions countering behavioural distortion and addresses the issue of privacy consent evidencing, on one side, the interest of online users in personalised information, including targeted advertisement, and, on the other side, the possibility to maintain that any privacy consent given for a processing activity that is either directly or indirectly prohibited by mandatory provisions of Union or national law shall be deemed invalid pursuant to article 5(1)(b) GDPR, remarking that this interpretation of the GDPR helps in overcoming a procedural interpretation of the controller's accountability principle, rightly criticised by Ignacio Cofone in his book.

L'autore offre alcune osservazioni su "The Privacy Fallacy" di Ignacio Cofone in relazione a una selezione di disposizioni imperative del diritto dell'Unione europea volte a contrastare la distorsione comportamentale e affronta la questione del consenso privacy, *evidenziando, da un lato, l'interesse degli utenti online a ricevere informazioni personalizzate, compresa la pubblicità mirata, e, dall'altro, la possibilità di sostenere che qualsiasi consenso privacy fornito per un'attività di trattamento direttamente o indirettamente vietata da disposizioni imperative del diritto dell'Unione o nazionale sia da considerarsi invalido ai sensi dell'articolo 5, par. 1, lett. b), GDPR, sottolineando che questa interpretazione del GDPR contribuisce a superare un'interpretazione procedurale del principio di responsabilità del titolare del trattamento, giustamente criticata da Ignacio Cofone nel suo libro.*

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: privacy consent; behavioural distortion; personalised information

Summary: 1. Introduction. – 2. The myth of rationality and a 20th birthday. – 3. The myth of apathy and a lunch invitation. – 4. The provisions of contemporary data law laying down direct or indirect prohibitions on personal data processing and the invalidity of privacy consent for illegitimacy of the processing purposes. – 5. The invalidity of Mr. Leon's consent to the processing of his personal data for the purpose of making him the target of an aggressive commercial practice. – 6. Relational nature of data. – 7. Characters of new EU data law. – 8. Conclusive remarks.

1. Introduction.

To start with, I would like to thank Ignacio Cofone and Lucilla Gatt for having invited me to take part to this initiative. *The Privacy Fallacy*[1] offers many ideas for discussing the adequacy of the traditional model of privacy protection – and I would say: for more broadly rethinking the traditional model of online users' protection - in the contemporary world characterised by the spread of large digital platforms and artificial intelligence applications.

Among the many reflections triggered by the reading of *The Privacy Fallacy*, I will focus on the topics discussed by the author in the parts of the book dedicated to the 'myth of rationality' and the 'myth of apathy',[2] as well as on some ramifications of his discussion about the relational nature of personal data.[3]

I will briefly comment about these three issues, proposing - in line with the very interesting analysis made by Ignacio Cofone and his mindful remarks - some further elements of discussion with the benefit of the elaboration of certain categories and concepts of EU contemporary data law in combination with a critical review of some fundamental principles of EU consumer law.

In accepting the opportune invitation by Cofone to consider 'the way ahead', I will highlight some aspects of Union law that – in my opinion – should be taken into account for addressing and possibly resolving some of the most profound concerns highlighted in *The Privacy Fallacy*, by way of advocating new (as opposite to traditionalist) interpretations of existing EU privacy law provisions, starting from the GDPR, in combination with the many new sources of EU data law that have been introduced in the last five years or so.

The Privacy Fallacy is very clearly divided into two parts. In a first part - which we can define as *pars destruens* – the Author examines the limits of the traditional model of privacy protection based on the category of consent – a model defined in short by Cofone as the contract law model – in order to propose the tort law model as an alternative model (*pars construens*).

Discussing the *pars destruens*, the author speaks of the 'myths' of 'rationality' and 'apathy', to indicate, respectively, the fallacy of the belief according to

[1] I Cofone, *The Privacy Fallacy. Harm and Power in the Information Society* (Cambridge University Press 2024).
[2] Chapter 2.
[3] Page 50 ff.

which people would generally make rational choices provided that they have all the relevant information to make an informed decision; and the fallacy of the belief according to which people, in the alternative between worrying and not caring about privacy, would generally tend not to care about privacy. This alleged situation is also referred to as the "privacy paradox" by many other authors. As I will discuss further, a third option may be factored in in the analysis, in addition to the alternative between worrying and not caring about privacy, consisting in an aware and positive attitude by online users to provide personal data precisely with the expectation of receiving personalised communication (see paragraph 3 below).

2. The myth of rationality and a 20th birthday.

Although not always acknowledged by scholars and hardly recognized by the European Court of Justice (ECJ) (see *infra* in this paragraph), exactly 20 years ago, with the introduction of directive 2005/29/EC (UCPD),[4] EU consumer law eradicated the 'myth of rationality', ie the wrong belief according to which people would generally make rational choices provided that they have all the relevant information to make an informed decision.[5] In the year of its 20th birthday, it is time to recognize the importance and centrality of UCPD in Union law precisely for this reason.

To remark and argue on this point is certainly relevant also for discussing the issue of consent to the processing of personal data in the contemporary data driven society, where online users are most often consumers and their online

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

[5] For a view expressed in 2015 that the ECJ has a tendency towards viewing the average consumer as a rational decision-maker, see BB Duivenvoorde, 'The Average Consumer Benchmark From a Behavioural Perspective', in *The Consumer Benchmarks in the Unfair Commercial Practices Directive*, Studies in European Economic Law and Regulation (Springer, 2015) vol. 5. Similarly, in an essay of 2011 it was noted by Jan Trzaskowski that the interpretation by the ECJ of the concept of average consumer used in the UCPD is that of the *homo economicus* (J Trzaskowski, 'Behavioural Economics, Neuroscience, and the Unfair Commercial Practises Directive', (2011) 34 JCP 377 ff. see in particular 390-391. At the same time the author expressed the opinion that the UCPD can *and should* be interpreted differently, and that the average consumer test required by the UCPD «is flexible enough to allow the inclusion of research within human decision-making in order to apply a more realistic average consumer than the currently applied *Homo Economicus*» (391). See also: Id., 'Behavioural Innovations in Marketing Law'*, in* H. Micklitz, A-L. Sibony , F. Esposito (eds) *Handbook of Research Methods in Consumer Law* (Edward Elgar, 2018) 296 ff.; Id., 'Interpretation and Assessment under the Unfair Commercial Practices Directive — the ICC Code for Advertising and Marketing and the Commission's Staff Working Document*',* in U. Bernitz, C. Heide-Jørgensen (eds), *Marketing and Advertising Law in a Process of Harmonization* (Hart Publishing, 2017) 85 ff.; Id., 'Lawful Distortion of Consumers' Economic Behaviour – Collateral Damage Under the Unfair Commercial P ractices Directive'(2016) 1 Eur Bus L Rev, 25 ff. An analysis of how behavioural insights could be used to shape the interpretation of European law on unfair practices is given by A Sibony, 'Can EU Consumer Law Benefit From Behavioural Insights?', in K. Mathis, *European Perspectives on Behavioural Law and Economics. Economic Analysis of Law in European Legal Scholarship* (2nd ed., Springer 2015) vol. 2.
We shall comment further in this paragraph the most recent judgment Case C-646/22 Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (AGCM) of the Court (Fifth Chamber) of 14 November 2024

decisions relevant to the processing of their personal data are most often of an economic nature because of the so called 'monetization' of personal data.

As we will also discuss in paragraph 3 below, Union law has undoubtedly recognized the remunerative function of personal data.

Before and after the Data Content Directive of 2019 (DCD),[6] whose article 3(1)[7] triggered a large debate a few years ago, a number of other EU normative acts have been introduced that contemplate either the provision of personal data in terms of remuneration, or contracts for the supply of personal data in exchange for money or for altruistic purposes, including:

- the recast directive of 2018 (predating the DCD) establishing the European Code of Electronic Communication;[8]
- the so-called Enforcement and Modernization (or Omnibus) directive of 2019;[9]
- the Data Governance Act of 2022 (DGA);[10] and

[6] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. [2019] OJ L136/1.

[7] Art. 3(1) DCD: «This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price. This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose».

[8] Although the DCD is commonly referred to as the first normative act of Union law recognizing the remunerative function of personal data, recital 16 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) already stated as follows: «In order to fall within the scope of the definition of electronic communications service, a service needs to be provided normally in exchange for remuneration. In the digital economy, market participants increasingly consider information about users as having a monetary value. Electronic communications services are often supplied to the end-user not only for money, but increasingly and in particular for the provision of personal data or other data. The concept of remuneration should therefore encompass situations where the provider of a service requests and the end-user knowingly provides personal data within the meaning of Regulation (EU) 2016/679 or other data directly or indirectly to the provider. It should also encompass situations where the end-user allows access to information without actively supplying it, such as personal data, including the IP address, or other automatically generated information, such as information collected and transmitted by a cookie. In line with the case-law of the Court of Justice of the European Union (Court of Justice) on Article 57 TFEU (16), remuneration also exists within the meaning of the TFEU if the service provider is paid by a third party and not by the service recipient. The concept of remuneration should therefore also encompass situations in which the end-user is exposed to advertisements as a condition for gaining access to the service, or situations in which the service provider monetises personal data it has collected in accordance with Regulation (EU) 2016/679».

[9] Article 4(2)(b) of directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, [2019] OJ L328/7 (so-called *Omnibus* or *Enforcement and Modernization* directive) has amended article 3 of directive 2011/83/EU on consumer rights by way of inserting the following paragraph 1a «This Directive shall also apply where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content which is not supplied on a tangible medium or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose».

[10] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] L152/1. See definitions of *data sharing*, of *data intermediation service* and *data altruism* under article 2, numbers 10, 11 and 16 DGA.

- the Data Act of 2023 (DA).[11]

In paragraph 4.2.7, titled Data-driven practices and dark patterns, of the Commission's Guidance on the interpretation of the UCPD published in December 2021,[12] it is noted as follows: «The UCPD covers the advertising, sales and contract performance stages, including the agreement to the processing of personal data and the use of personal data for delivering personalised content, and the termination of a contractual relationship. The directive has a broad scope of application: it covers all business-to-consumer commercial practices and does not require the existence of a contractual relationship or the purchase of a product. For example, the Directive would also cover commercial practices such as capturing the consumer's attention, which results in transactional decisions such as continuing to using the service (e.g. scrolling through a feed), to view advertising content or to click on a link».

UCPD deals with consumer marketing,[13] i.e. with commercial practices that are aimed at influencing consumers' economic behaviour[14] and provides criteria to distinguish between "influencing" and "distorting" consumers' behaviour. Influencing consumers' decisions is not per se prohibited. To give a pair of indisputable examples: advertising and marketing in general are not prohibited *as such*. The purpose of the UCPD is precisely that of fixing general criteria for establishing upon which conditions influencing is legitimate ('fair') and upon which conditions it becomes illegitimate ('unfair').

[11] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending regulation (EU) 2017/2394 and directive (EU) 2020/1828 (Data Act) [2023] OJ L 22/12/2023. See articles 9 (*Compensation for making data available*) and 13 (*Unfair contractual terms unilaterally imposed on another enterprise*) DA.

[12] Commission Notice 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 [2021] OJ C526/1. See F Di Porto, A Egberts, 'The collective welfare dimension of dark patterns regulation', (2023) 19 (1-2) *European Law Journal*, pp. 114-141.

[13] Marketing activities are designed to influence the behaviour of a stated target to obtain certain behavioural answers. See *ex multis*: P. Kotler, K. Keller, A. Chernev, *Marketing Management. Global Edition* (16th edn Pearson, 2021) 29 ff.; P. Kotler, K. Keller, *Marketing management* (12th edn, W. G. Scott 2006), Italian translation by F Sarpi, Milan, 2007, 7- 10; P. Kotler, J. Armstrong, V. Wong, J. Saunders, *Principles of marketing* (5th edn, Pearson, 2008); P. Kotler, S. Hollensen, M. O. Opresnik, *Social media marketing, Marketer nella rivoluzione digitale* (Hoepli 2019).

[14] The subject matter of the discipline consists not of all the commercial practices responding to the definition of art 2(d) UCPD, but *only* of any such commercial practices that can influence the consumer's economic behaviour. This concept is clearly expressed in general terms in the subsequent recital 7: «This Directive addresses commercial practices directly related to influencing consumers' transactional decisions in relation to products». The drafters of the directive have proceeded on the basis of the observation of the advertising and marketing practices existing in the market, and in particular the consideration that such practices are by their nature aimed at influencing the economic behaviour of consumers, and that, upon certain conditions, this aim can be legitimately pursued. This is clearly stated in recital 6 «[…] this Directive does not affect accepted advertising and marketing practices, such as legitimate product placement, brand differentiation or the offering of incentives which may legitimately affect consumers' perception of products and influence their behaviour without impairing the consumer's ability to make an informed decision».
From this recital we can see that, not only does the directive not prohibit many advertising and marketing practices that can influence consumers' economic behaviour, but more significantly we can appreciate that the directive intends to regulate advertising and all other marketing practices precisely because they have such orientation and capacity. In other words, the drafters of the UCPD made it clear that they had precisely considered the current character of marketing and advertising practices as a set of activities, procedures and means effectively aimed at influencing consumers' transactional decisions and had decided to regulate such practices.

The focus of the UCPD has been set in the decision-making process of consumers, through the concept of consumer's transactional decision. The concept of average consumer and that of average member of a group of consumers have been used. These concepts, far from being simplistic (as often taught),[15] require the interpreter to consider certain average consumer's conditions of vulnerability associated with the consumer's decision-making process.

The type of average consumer that is reasonably well-informed and reasonably observant and circumspect is not at all simplistic, while it is a precise legal concept that interpreters need to look at *a contrario*, in order to capture the average conditions of corresponding vulnerabilities. In the case of information, it is ignorance. As Blaise Pascal used to say, knowledge and ignorance coexist in anyone (anyone's vast ignorance has a few gaps) and marketers very well know how to exploit ignorance. The same applies to the conditions of observance and circumspection. They too shall be read *a contrario* in terms of average conditions of lack of observance and circumspection.

Acting in a manner contrary to the requirements of professional diligence, in the sense intended by the UCPD, essentially means acting in a way that allows the trader to take advantage of certain average consumer's conditions of vulnerability associated with the consumer's decision-making process, ie with average conditions of behavioural or decisional vulnerability. In essence, it is forbidden to influence consumers' transactional decisions in such a way as to take advantage of certain average consumer's conditions of decisional/behavioural vulnerability. Whenever the trader puts in place commercial practices that present this feature, he is said to 'distort' (as opposite to 'influence') the consumers' economic behaviour, and, in brief, to act unfairly.[16]

The revolutionary step forward made by the UCPD with respect to prior legislation against misleading advertising, consists in having laid down not only provisions against practices that prevent consumers to make informed decisions ('misleading' practices) but also provisions against practices that prevent consumers from making free decisions ('aggressive' practices).

In putting forward the category of 'aggressive commercial practices', the UCPD has overcome the model of protection of the *homo economicus* (the model of man that only needs critical information to make rational decisions)

---

[15] See, G Helleringer , A L Sibony, 'European Consumer Protection through the Behavioral Lens'(2016) 23, Colum J Eur L, 607 ff., 617 where the opinion is also expressed that EU consumer law has evolved into an apparent anti-model of behavioral regulation; P Cartwright, 'The Consumer Image Within EU Law', in C. Twigg-Flesner, *Research Handbook on EU Consumer and Contract Law* (Edward Elgar, 2016) 204 ff; S Weatherhill, 'Who is the "Average Consumer"?', in S. Weatherhill , U. Bernitz (eds) *The Regulation of Unfair Commercial Practices under EC Directive 2005/29: New Rules and New Techniques* (Hart, 2007); R Incardona, C Poncibò, 'The average consumer, the unfair commercial practices directive, and the cognitive revolution' (2007) 30 J Cons Pol, 21 ff, where the opinion is expressed that the average consumer is an overly simplistic concept with little correspondence with the real world of individual consumer behaviour and should be reinterpreted more flexibly, or even abandoned to mirror consumer behaviour more effectively.

[16] See extensively, S Orlando, 'The Use of Unfair Contractual Terms as an Unfair Commercial Practice'(2011) 1, Eur Rev Contract L, 39 ff.; B Parenzo, 'Neuromarketing: un inventario di (spuntati) divieti contro il pericolo di una scelta manipolata', in S. Orlando (ed) *Profili giuridici del neuromarketing. Annuario 2023–2024 OGID Osservatorio Giuridico sull'Innovazione Digitale* (1st ed., 2025), 261 ff.

to pioneer a model of protection that embraces the results of behavioural economics.[17]

The (right) assumption of the UCPD is that information is not the only driver to consumers' decisions, and that many other drivers exist, including of a psychological and emotional nature, that may be exploited fairly or unfairly by traders.

Reference to 'professional diligence' is made in the UCPD exactly for this purpose and it has a central role in understanding the concept of average consumer and to make it function for the purposes of the directive. The European legislator considered the indisputable fact that traders study their targets in order to figure out how to best influence them, and that, for the same reason, they also know their targets' behavioural vulnerabilities.[18] In making reference to professional diligence, therefore, the UCPD prescribes that traders shall observe a professional duty of care, deriving from this knowledge. Conforming to professional diligence in this specific context of professional activity consisting of influencing consumer's behaviour means that traders shall observe that duty of care: they have to care about consumers' behavioural vulnerabilities, which means that traders shall refrain from exploiting those vulnerabilities.

If this is understood, it appears correct to say that the parameter of the average consumer is not external from but is indeed inherent to the notion of professional diligence, in the sense that the 'contrariety to the requirements of professional diligence' shall be construed in theoretical terms and assessed in practice precisely in relation to the parameter of the average consumer (or to the average member of a group of consumers), and more specifically in relation to certain average subjective conditions of decisional vulnerability to certain

[17] See authors quoted in footnote 5 above. For an extensive study about research in consumer law and behavioural sciences, see F Esposito, 'Conceptual Foundations for a European Consumer Law and Behavioural Sciences Scholarship', in H. W. Micklitz, A. L. Sibony, F. Esposito (eds) *Research Handbook in Consumer Law* (Edward Elgar, 2018) 38 ff.

[18] Article 5(2) UCPD literally establishes two separate constitutive elements for unfairness: the contrariety to the requirements of professional diligence *and* the ability to materially distort the consumers' economic behaviour. However, this is simply due to the approach followed by the legislator in providing the definition of commercial practices. If we adhere to the interpretation, herein supported, according to which the commercial practices that form the subject matter of the discipline are 'commercial practices' (according to the definition of art 2 (d) of the UCPD) that are further able to influence consumers' economic behaviour (recital 7 of the UCPD), we also appreciate that the two elements should be merged into one. And effectively – even without considering how hard it would be to adhere to the proposition that a commercial practice which can materially distort the economic behaviour of the average consumer may be compliant with the requirements of professional diligence, thus qualifying as fair, which possibility would have to be contemplated were one to accept that the two elements are separate – the definition of 'professional diligence' contained in art 2 (h) as well as the spirit and the ultimate goal of the discipline support the above conclusion. The first observation is that the definition-formula of 'professional diligence' makes clear that the trader has *a duty of care towards consumers*. The second observation is that the trader's duty of care toward consumers should be set in relation to 'honest market practices and/or the general principle of good faith', and that the reference contained (in the same definition formula) to the 'trader's field of activity' requires the interpreter to put 'honest market practices and/or the general principle of good faith' in context. Putting in context honest market practices and/or the general principle of good faith in relation to the trader's field of activity means that the guiding principles of honest market practices and/or good faith shall be applied, taking into account not only the nature of the commercial practice from time to time under scrutiny and the features of the relevant product, but also the target or targets of consumers interested by the same practice, since any such target essentially characterises the 'trader's field of activity' and also essentially characterises the commercial practice, allowing the interpreter to capture the quality critical for the purposes of the discipline in question, ie its influential capacity.

practices, of consumers to which the practices are addressed. Vulnerability is a relational concept: one is vulnerable *to* something, which means - in the context of the UCPD - to certain practices.[19] Some people are vulnerable to certain practices and not to others depending on their subjective conditions of vulnerability. For the same reasons, people may be targeted and grouped depending on their average conditions of vulnerability to certain influential practices. This is how the concept of 'group of consumers' in the UCPD shall be intended.

To state which average conditions of vulnerability are precisely relevant for the UCPD is a matter of interpretation. In many provisions, the UCPD clearly states the concept of decisional vulnerability in general terms and also makes clear that average conditions of decisional vulnerability are relevant.[20] As said, the directive expressly mentions information, observance and circumspection.[21] These subjective conditions are such that, by taking advantage of the same (e.g. of the lack of information of the average consumer or of the average member of a given group of consumers to which the practice is addressed), the trader impairs the average consumer's awareness in the making of a transactional decision. However, these are not the only subjective conditions of vulnerability relevant for the UCPD, because others exist and are critical for assessing whether the average consumer is potentially impaired in his freedom (as opposite to awareness) in making a transactional decision. This observation is based on the interpretation of the definition of 'aggressive commercial practices'.[22] The nature of aggressive practices and of their statutory forms (consisting of 'harassment', 'coercion' and 'undue influence') requires the interpreter to make reference to a judgement of vulnerability as measured against different average subjective conditions, such as the consumer's impressionability and the consumer's ability to resist and to react, which may in turn depend on average conditions of information, observance, and circumspection, but may also be completely independent of the latter.[23]

The 'misleading' practices are contrary to the professional diligence – and are therefore forbidden by the UCPD – because, and insofar they exploit information vulnerability of consumers, ie the so-called information asymmetry typically characterising many relations between traders and consumers, as well as other vulnerability conditions pertaining more generally to the ability of the

[19] Recital 18 UCPD.
[20] Art. 5(3) and recital 18 UCPD.
[21] Recital 18 of the UCPD.
[22] Articles 8 and 9 UCPD.
[23] More precisely, in respect of commercial practices the nature of which as harassment should be established, the critical subjective conditions relevant to the test of average vulnerability will be those of the ability to resist and the ability to react. On the basis of 'average' psychological or economic abilities of resistance and reaction it will have to be assessed whether the practice qualifies as harassment, ie whether the commercial practice is able to significantly impair the average consumer's freedom of choice or conduct. An affirmative answer will be given even in those cases where it is judged that the average consumer is well-informed about his right to resist or react to the harassment. Similar considerations seem to apply in relation to aggressive commercial practices consisting of coercion and undue influence. In particular, it seems appropriate to observe that the subjective condition relevant for coercion is that of the 'impressionability' (rather than those of information, observance and circumspection); similarly, a consumer, despite being reasonably well-informed and reasonably observant and circumspect, may nevertheless be impaired in his freedom of choice or conduct by commercial practices consisting of undue influence, depending on his abilities to resist and react to the pressure exercised by the trader in the exploitation of a position of power vis-à-vis the consumer (art 2 (j) of the UCPD).

consumer to acquire under the circumstances (time, space, communication context and composition) knowledge and awareness of all the information critical for the making of a transactional decision, consisting in average conditions of cognitive vulnerability such as average lack of attention and circumspection that can be exploited by traders in many ways including through presentational features of the communication.[24] Cognitive vulnerabilities are often referred to in terms of cognitive bias and they are about the formation of awareness by consumers.

The 'aggressive' practices are contrary to the professional diligence – and are therefore forbidden by the UCPD – because, and insofar they exploit vulnerabilities of other kinds, including emotional and psychological vulnerabilities independently from any lack of relevant information by the consumer, and even in cases in which the consumer has all the awareness and information necessary to make a transactional decision. Therefore, they are different from cognitive vulnerabilities. Subjective conditions of vulnerability associated with aggressive marketing practices consist in average lack of capacity to resist or to react and impressionability. Marketing aggressive practices successfully exploiting these vulnerabilities make consumer take decisions that he would not have taken otherwise, even in the awareness by the consumer of his rights and of all factual circumstances that are critical for his choice.

Two examples of aggressive commercial practices exploiting, respectively, average conditions of lack of capacity to resist or react, and impressionability, are that of failing systematically to respond to pertinent correspondence in order to dissuade consumers from exercising their contractual rights,[25] and that of creating the impression that the consumer cannot leave the premises until a contract is formed.[26]

These two examples not only are very clear about the nature of the vulnerabilities concerned and their difference with respect to those of a cognitive or informative nature, typical of the misleading practices, as said, but they are also very instructive as to how low the threshold is, according to the UCPD, to establish that a marketing practice is 'aggressive'. In fact, the level of intensity of 'coercion' 'harassment' and 'undue influence' (i.e. the three concepts for defining 'aggressive commercial practices', under the UCPD)[27] that are needed for determining whether a certain marketing practice shall qualify as 'aggressive' pursuant to the UCPD, under the circumstances, may and

[24] Recital 18 UCPD. I do not agree with the opinion expressed in the above quoted essay by G Helleringer, A Sibony 'European Consumer Protection through the Behavioral Lens' (2016) 23 Colum. J. Eur. L 623 , according to which UCPD would not prohibit «confusing information overload», as information overload may well be prohibited precisely for being confusing (deceptive), in all cases in which, under the circumstances, it would result in exploiting consumers' average conditions of lack of observance and circumspection so as to impair the ability of an average consumer to take an informed decision. In this respect, it appears worth pointing out that art. 6(1) UCPD expressly takes into account presentational features of factually correct (thus also complete) information characterizing misleading actions: «A commercial practice shall be regarded as misleading if […] in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct […]».

[25] UCPD: point 27 of Annex I.

[26] UCPD: point 24 of Annex I.

[27] Articles 2(j), 8 and 9 UCPD.

shall be derived by examining the list of typically aggressive practices contained in Annex I to the UCPD.

The second example is also particularly significant and useful for introducing the item of the so-called dark patterns. The aggressive commercial practice consisting in creating the impression that the consumer cannot leave the premises until a contract is formed is an unfair practice "designed architecturally", as it typically results from an architectural solution that force all people that want to leave the premises of a commercial centre, even those who do not make a purchase, to stand in the checkout line used by the customers that have to wait to pay at the checkout counter.

Much like the architectural design of a physical space, the software design of online interfaces may result in unfairly influencing users' behaviour, i.e. to produce behavioural distortions on online users. The Digital Services Act (DSA)[28] contains a prohibition that precisely uses this concept: «providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions» (article 25(1) DSA).[29]

In the recitals of the DSA,[30] the explanation of this prohibition is provided by using the expression 'dark patterns' which was firstly adopted in the US in 2010 and subsequently changed into 'deceptive design patterns'.[31] Despite the success that this expression has gained also in Europe,[32] it is very important, as

[28] 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). [2022] OJ L 277/1

[29] Article 25(1) DSA.

[30] Recital 67 DSA: «Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them. Providers of online platforms should therefore be prohibited from deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof. This should include, but not be limited to, exploitative design choices to direct the recipient to actions that benefit the provider of online platforms, but which may not be in the recipients' interests, presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory, or other components, when asking the recipient of the service for a decision. It should also include repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, making the procedure of cancelling a service significantly more cumbersome than signing up to it, or making certain choices more difficult or time-consuming than others, making it unreasonably difficult to discontinue purchases or to sign out from a given online platform allowing consumers to conclude distance contracts with traders, and deceiving the recipients of the service by nudging them into decisions on transactions, or by default settings that are very difficult to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice. However, rules preventing dark patterns should not be understood as preventing providers to interact directly with recipients of the service and to offer new or additional services to them […]».

[31] https://www.deceptive.design/

[32] The expression 'dark patterns' has been widely used in official documents of EU institutions, and in a number of studies commissioned by EU institutions as well as by institutions and authorities of Member States, including *ex multis* in: recital 67 of the Digital Services Act; the already quoted Commission Notice *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* (2021)OJ C 526/1; the first version (for public consultation) of the EDPB *Guidelines n. 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them* of 21 March 2022 (the final version, version 2.0 adopted on 14 February 2023 was renamed as: *Guidelines n. 3/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them*); in a document containing the results of a screening ("sweep") of retail websites addressing manipulative online practices, published on 30 January 2023 by the

a matter of EU law, to recognize that the concept of behavioural distortion was introduced in Union law by the UCPD in 2005, and that this concept and the relevant categories of decisional or behavioural vulnerabilities are those relevant as a matter of Union law:[33]

Similarly, article 13(6) of the Digital Markets Act (DMA),[34] contains a prohibition for gatekeepers on making the exercise of certain rights or choices of end users or business users «unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof».

The importance and centrality of the concept of behavioural distortion introduced by the UCPD is confirmed by article 5 of the Artificial Intelligence Act (AI Act or AIA),[35] which puts forward some prohibitions on commercializing

European Commission and national consumer protection authorities of 23 Member States, Norway and Iceland (CPC Network); the study commissioned by the European Commission: Directorate-General for Justice and Consumers: F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, Final Report of April 2022, (https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418); the Guidelines issued by the Dutch Authority for Consumers and Markets (ACM) on 11 February 2020, titled *Protection of the online consumer – Boundaries of online persuasion* (https://www.acm.nl/en/publications/guidelines-protection-online-consumer); the study published by the Bureau Européen des Unions de Consommateurs (BEUC) titled *"Dark Patterns" and the EU Consumer Law Acquis– Recommendations for better enforcement and reform*, of 7-9 February 2022 (https://www.beuc.eu/position-papers/dark-patterns-and-eu-consumer-law-acquis); the study of 2018 published by the Norwigian Consumer Council titled (in the English version) *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf); the study published by the French Data Protection Authority (CNIL) and writtend by an independent study group (Foresight) in 2019, titled (in the English version) *Shaping Choices in the Digital World. From dark patterns to data protection: the influence of UX/UI design on user empowerment*, (https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf).

[33] C Isola,F Esposito, 'A systematic literature review on dark patterns for the legal community: definitioal clarity and a legal classification based on the Unfair Commercial Practices Directive'(2025) 58, Comput L Secur Rev, 106 - 169; S Orlando, 'A proposito dei deceptive design (già dark) patterns', in G. Grisi, S. Tommasi (eds) *Mercato digitale e tutela dei consumatori. Prove di futuro* (Giappichelli 2024). 63 ff.; F Esposito,TMC Ferreira, 'Addictive Design as an Unfair Commercial Practice: The Case of Hyper Engaging Dark Patterns'(2024)15 Eur J Risk Regul, 999 ff. The assertion that dark patterns have a general relevance in consumer law in terms as unfair commercial practices is made clearly, as noted, in paragraph 4.2.7 of the Commission Notice Guidance 2021/526 on the interpretation of the UCPD. The same assertion is made in the abovementioned Guidelines of the Dutch Authority for Consumers and Markets (ACM) of 11 February 2020, wherein, at page 52, the following definition of dark patterns is contained «User interfaces (also: UI) that have been designed in such a way that they exert negative influence on the user and cause them to take a decision desired by the designer. Dark patterns can constitute unfair commercial practices. Unfair commercial practices are not permitted. These guidelines provide a basis for assessing whether practices are unfair», as well as in the already quoted and very significant Final Report of 20 April 2022 published by the European Commission, titled *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization*.

[34] 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). [2022], OJ L 265/1

[35] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 12/07/2024.

and operating AI systems that are able to distort human behaviour and cause significant harm to people.[36]

Finally, a number of other recent provisions of Union law, although not directly laying down prohibitions on distorting people's behaviour, clearly are instrumental to the purpose of preventing behavioural distortion, such as those contained in articles 26(4)[37] and 28(2)[38] DSA, article 18(1)(c) of regulation (EU) 2024/900 on transparency and targeting of political advertising,[39] article 10(5)

[36] According to article 5(1)(a) and (b) AI Act it shall be prohibited the placing on the market putting into service and use of:
(a) AI systems that «[deploy] subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm»; and *(b)* AI systems that «[exploit] any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm».
See *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, published on 4 February 2025 (https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act).
[37] Art. 26(4) DSA: «Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679».
[38] Art. 28(2) DSA: «Providers of online platforms shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor».
[39] Art. 18(1)(c) reg. (EU) 2024/900: «Targeting techniques or ad-delivery techniques that involve the processing of personal data in the context of online political advertising shall be permitted only when the following conditions are fulfilled: […] those techniques do not involve 'profiling' as defined in Article 4, point 4, of Regulation (EU) 2016/679 and in Article 3, point 5, of Regulation (EU) 2018/1725 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679 and in Article 10(1) of Regulation (EU) 2018/1725».

of the AI Act[40] and article 54(c) of the recently adopted regulation on the European Health Data Space (EHDS Regulation).[41][42]

The problem appears to be more of an interpretative nature, since it is still not widely recognised that it was UCPD to have archived 20 years ago the model of *homo economicus* as the only model of consumer worth of legal protection in Union law, and, as a consequence, the potential for the revolutionary reach of UCPD has not been fully exploited yet.[43]

Some interpretative effort is needed also on account of the wording of the UCPD. The UCPD itself, in the definitions of 'to materially distort the economic behaviour of consumers' and of 'undue influence' only refers literally to the impairment of the consumer's ability to make an informed decision"[44] but those definitions certainly shall be interpreted as reading «free and informed decision», on account of the fact that UCPD's provisions against aggressive commercial practices certainly protect free decisions, as reminded above. Indubitably, art. 8 UCPD defines 'aggressive commercial practice' by the fact that it impairs or is likely to significantly impair the average consumer's freedom of choice or conduct.[45]

Also, the recent decision by the ECJ in the Compass case C-646/22,[46] although recognising that under the UCPD the concept of average consumer

[40] Art. 10(5) AI Act: «To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, all the following conditions must be met in order for such processing to occur: (a) the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data; (b) the special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation; (c) the special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations; (d) the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties;(e) the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first; (f) the records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data».

[41] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, [2025], OJ L 5.3.2025

[42] Article 54, letter c) of the EHDS Regulation prohibits the secondary use of electronic health data consisting in «carrying out advertising or marketing activities».

[43] J Trzaskowski, 'Behavioural Economics, Neuroscience, and the Unfair Commercial Practises Directive' (2011)34, J Cons Pol, 390-391

[44] Art. 2(e) and (j) UCPD.

[45] Art. 8 UCPD «A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise».

[46] ECJ Judgment of the Court (Fifth Chamber) of 14 November 2024 - Compass Banca, C-646/22 EU:C:2024:957.

does not correspond to that of *homo oeconomicus*, still limited its analysis to the possible impact of cognitive biases.[47]

Cognitive biases affect the ability of consumers to be fully aware, ie to acquire all the information necessary for making a transactional decision under the circumstances. Cognitive biases may be associated to subjective conditions of vulnerability such as lack of information as well as lack of observance and circumspection that may very well be exploited by marketers. However, as said, other kinds of vulnerabilities exist such as those consisting in the lack of capacity to resist or react, or in impressionability, that too are typically exploited through unfair marketing practices, in particular through aggressive marketing practices, and which certainly are able to distort consumers' behaviour: pressing consumers to make certain decisions despite their complete and full knowledge of all the facts critical for their choice, i.e. in the absence of any cognitive biases.

As said, this is the case, for example, of the decision not to exercise a contractual right as a consequence of the aggressive practice listed in point 27 of Annex I of the UCPD.[48] In that case, typically the consumer is fully aware of his/her rights (no cognitive biases) but still takes a decision that he/she would not have taken otherwise.

That said, it also appears necessary to make some progress in the interpretation and application of the UCPD so as to propose interpretations of the directive that are adequate ad adapted at current times, having regard to the features of contemporary marketing, precisely because – as said – marketing practices form the subject matter of the UCPD.

In particular, it appears necessary to elaborate interpretations of the UCPD adequate to the contemporary techniques of neuromarketing[49] and personalised marketing.[50] These two fields of application of the UCPD are at

[47] Point 59 of ECJ Judgment of the Court (Fifth Chamber) 14 November 2024 - Compass Banca, C-646/22: «Directive 2005/29 must be interpreted as meaning that the concept of 'average consumer', within the meaning of that directive, must be defined by reference to a consumer who is reasonably well-informed and reasonably observant and circumspect. Such a definition does not, however, exclude the possibility that an individual's decision-making capacity may be impaired by constraints, such as cognitive biases».

[48] UCPD, point 27 of Annex I: «Requiring a consumer who wishes to claim on an insurance policy to produce documents which could not reasonably be considered relevant as to whether the claim was valid, or failing systematically to respond to pertinent correspondence, in order to dissuade a consumer from exercising his contractual rights».

[49] F Bertelli, 'Consumer Education in the Digital Era: Re-shaping the Vulnerable, the Average and the Informed Consumer?', in S. Orlando (ed) *Profili giuridici del neuromarketing. Annuario 2023–2024 OGID Osservatorio Giuridico sull'Innovazione Digitale* (Roma Sapienza Università Editrice, 2025) 25 ff.; L Sposini , 'Consumer Protection in the Age of Biotechnology and Artificial Intelligence: The Case Study of Neuromarketing and the Exploitation of Human Biases', in S. Orlando (ed) *Profili giuridici del neuromarketing. Annuario 2023–2024 OGID Osservatorio Giuridico sull'Innovazione Digitale* (Roma Sapienza Università Editrice, 2025), 279 ff.

[50] See Commission Notice Guidance 2021/C 526/01, par. 4.2.7: «Traders can develop personalised persuasion practices because they benefit from superior knowledge based on aggregated data about consumer behaviour and preferences, for example by linking data from different sources. Traders can also have the possibility to make adjustments to improve the effectiveness of their practices, as they continuously test the effects of their practices on consumers and thereby learn more about their behaviour (e.g. through A/B testing). Furthermore, such practices could often be employed without the full knowledge of the consumer. It is the presence of these factors and their opaqueness that distinguishes, on the one hand, highly persuasive advertising or sales techniques from, on the other hand, commercial practices that may be manipulative and, hence, unfair under consumer law. […] For the purposes of this assessment, the benchmark of an average or vulnerable consumer can be modulated to the target group and, if the practice is highly personalised, even formulated from the perspective of a single person who was subject to the

the frontline if we want – as Ignacio Cofone opportunely suggested – look ahead.

As a separate matter, it should be recognised that the capacity/lack of capacity to resist and to react to a commercial practice relevant for the UCPD may be also of an economic (as opposite to psychological) nature, and that public enforcement measures of the UCPD are particularly adapt to counter practices that exploit vulnerabilities of this kind.

Finally, an overall reading of the many sources of EU law countering behavioural distortion clearly indicates, in my opinion, the shift from the era of consumer protection to the era of online user protection, in which provisions designed on the historic model of consumer law are elaborated to protect also online users other than consumers. As regards the issue of behavioural distortion, this novelty is particularly relevant in connection with the influential practices put in place by governments and public authorities. They too may influence citizens fairly or unfairly and the tendency to refer to governmental influential campaigns indistinctively in terms of 'nudging' is misleading as it hides the marketing nature of any influential practice. We live times in which we should be thankful for the existence (enforcement will have to be seen) of these provisions.

More generally, it is important to focus on the fact that online marketing is not confined to commercial communication but embraces all realms where an interest exists and techniques are put in place for influencing someone's behaviour. In addition to the well-known political marketing - which is considered not only by the already quoted EU regulation on transparency and targeting of political advertising [51] but also by the AI Act in connection with the development, commercialization and functioning of «AI systems intended to be used for influencing […] the voting behaviour» [52] - marketing practices are ordinarily put in place by non-profit organizations for attracting members and

specific personalisation. These practices may also have a more significant effect on vulnerable consumers. As explained in section 2.6, the characteristics that define vulnerability in Article 5(3) are indicative and non-exhaustive. The concept of vulnerability in the UCPD is dynamic and situational, meaning, for instance, that a consumer can be vulnerable in one situation but not in others. For example, certain consumers may be particularly susceptible to personalised persuasion practices in the digital environment, while less so in brick-and-mortar shops and other offline environments. The use of information about the vulnerabilities of specific consumers or a group of consumers for commercial purposes is likely to have an effect on the consumers' transactional decision. Depending on the circumstances of the case, such practices could amount to a form of manipulation in which the trader exercises 'undue influence' over the consumer, resulting in an aggressive commercial practice prohibited under Articles 8 and 9 of the UCPD. When assessing the presence of undue influence, according to Article 9(c) one should take into account the exploitation of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware».

[51] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, [2024], OJ L 20/03/2024

[52] Political marketing is considered in point 8(b) of Annex III of the AI Act, in connection with the use cases of AI systems that qualify or may qualify as "high risk" systems pursuant to article 6 AIA and that always are considered "high-risk" when carrying out profiling activity, pursuant to the GDPR's definition of profiling: «AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view».

donations,[53] as well as by organizations at large for influencing the behaviour of their employees or members (so-called 'internal marketing').

3. The myth of apathy and a lunch invitation.

In addition to the critical aspects investigated by Cofone in relation to the 'mith of apathy', it appears to be a good idea to investigate - outside of the binary choice between worrying and not caring about privacy - whether good reasons exist for people to give their consent to data processing.

Of course, we are confining our legal analysis to digital (or electronic[54]) data and – therefore – we need to focus on the legal relevance of the (never-ending) new applications of digital technologies.

In this respect, for correctly framing the discussion on privacy consent, it appears worth making some general remarks to the general assertion that legislators shall be up to date with technological innovation. Although that preposition is certainly true, it needs to be specified by adding that what legislators shall specifically consider - and what they do consider, as a matter of fact – is how new technological applications affect social relations. In other words, legislators shall not only understand technological changes (or they shall not study technological changes per se), but they shall specifically understand the social changes which are the consequence of technological changes.

As it happens in any field of law, also in the field of data law legislators must look at the expressions of sociality. Sociality is the synthesis between observed conduct and accepted conduct within a community; and it changes over time. The reason for historicity of law itself, in essence, is that sociality changes over time, as both the observed conduct and the accepted conduct within a community change over time.

Now, historicity of law is certainly an evident concept when addressing from a legal standpoint the contemporary phenomenon of monetization of personal data, which is at the root of all the concerns and questions brilliantly discussed in *The Privacy Fallacy*. The monetization of personal data is indeed such a new phenomenon that it even creates astonishment (the astonishment of history).

For a presentation that I made at the Rome's Capitolium at the official ceremony of the 25th year of establishment of the Italian data protection authority,[55] I used the following metaphor to demonstrate how sociality changes over time and can create astonishment, precisely regarding consent to personal data processing:

---

[53] The *International Review on Public and Nonprofit Marketing* edited by Springer, is a scholarly journal «dedicated to advancing knowledge in the areas of public, nonprofit, political, cause-related and social marketing». A number of articles on the impact guilt, shame and fear are published in reviews specialised in advertising and in non-profit marketing in particular.

[54] According to the definition of 'personal electronic health data' contained in art. 2(2)(a) of the EHDS Regulation, electronic data are data *processed in an electronic form*: («'personal electronic health data' means data concerning health and genetic data, processed in an electronic form»).

[55] S Orlando, 'La "monetizzazione" dei dati personali. Una prospettiva funzionale', in G Cerrina Feroni, *Il ruolo del Garante per la protezione dei dati personali. La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro* (Il Mulino 2023).

> A gentleman invites me for lunch: «come to my place tomorrow at lunch time, there will be many persons that you certainly wish to see, other people that you might want to know, and – aside – many others that pay me to observe you and learn something about you».

Until some years ago, most of the persons receiving an invitation of this kind would have certainly declined it, and not too kindly even. Today, a similar invitation is being accepted every day, every second by billions of people.

Faced with this reality, jurists comprehensibly tend to find a shield in fundamental rights. However, to be frank, any such attempt is per se incapable of explaining the reasons for the phenomenon. Fundamental rights certainly are needed for governing this phenomenon, however after having understood it.

Moreover, to underline the (indisputable) need for governing this phenomenon on the basis of fundamental rights is a fruitful exercise provided that it is made in the awareness of the double direction characterizing the interaction between Law and Society: if it is true that Law (through its action shaped in the first place on the models of fundamental rights) exercises a pressure of mandatory kind on Society, therefore acting to a certain extent in the direction of modelling people's conduct, it is also true that Society (through the continuous synthesis that the governed community makes within itself between the conduct observed and the conduct accepted by its members) exercises a pressure of effectiveness on Law, therefore shaping inevitably, to a certain extent, the models of rights and duties, including fundamental rights.

It is indeed undoubtable that all the questions that one may ask and all the answers that one may give concerning fundamental rights are historically conditioned.

Therefore, having acknowledged that in our discussion on privacy consent we cannot find recovery from History, we shall seek in the first place to understand the phenomenon, starting from the evaluation of the interests at stake, as is usually made in all legal analyses.

The metaphorical lunch invitation consists in an offer of a service without paying a price with money, which is made conditional upon the acceptance of a request to give consent to the collection and further processing of personal data of the invitee, so-called 'tying' and 'tied consent'.

The question that needs to be answered is: why billions of people every day, every second give a tied consent?

On the basis of the traditional framing of the discussion on privacy consent and, in particular, on the basis of the commonly accepted interpretation of article 7(4) GDPR[56] regarding its requirement of freedom (I make reference, in particular to the EDPB Guidelines 8/2020[57] and to the EDPB Opinion 8/2024[58]) any tied consent should always be either invalid or unexplainable.

[56] Art. 7(4) GDPR: «When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract».

[57] European Data Protection Board (EDPB) Guidelines 08/2020 on the targeting of social media users Version 2.0, adopted on 13 April 2021.

[58] EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, adopted on 17 April 2024.

And effectively, on the basis of the traditional interpretation that makes leverage on the fungibility or equivalence of the service offered in order to judge about the freedom of privacy consent, consent to data processing in 'tying' situations would either be explainable (the data subject gives his tied consent to benefit from a service without paying a price with money) but invalid (because, on the basis of that theory, any such consent would not be free by definition); or it would be valid (in those limited cases where the data subject has a real alternative possibility to benefit from an equivalent service provided by the same supplier of the service or by a third party without paying any price in money and without giving any tied consent) but unexplainable. And, in fact, why should one give his/her tied consent in the presence of a real alternative of an equivalent service without the request to pay a price in money or to give consent to the processing of his/her personal data?

We should therefore admit that, once the analysis is set on these terms, the phenomenon appears impossible to be explained in a plain and rational way.

To avoid this *cul-de-sac*, it appears necessary to be bold enough to reject the hypothesis that the interest in giving a tied consent always and exclusively consists in not paying a price in money for the service, and to consider that people may have an additional and good interest in giving a tied consent, further to the obvious one of not paying a price in money.

In this perspective, the need as a matter of logic arises to look at the specific purpose of the data processing as stated by the data controller. In particular, it appears necessary to assess whether - in giving a tied consent - the data subject may have an interest that can be typically satisfied through the realization of the specific purpose for which the personal data are being collected and processed. In carrying out an analysis of this kind, it is appropriate to reject in limine the idea that any additional interest of this type (additional to that of receiving a service without paying money) may consist in a generic interest to 'receive advertising'.

If we put our analysis in the right historical dimension, we will certainly realise that behavioural advertising and personalised marketing in general is not the dear old 'TV advertising' very typically unwanted and avoided by remote control from the sofa. Today, behavioural advertising, and, more generally, personalised marketing precisely is personalised communication.

It appears correct to say that an interest to receiving personalised information online may well typically exist, which is certainly not confined to straightforward advertising messages, but extends to and properly consists in the genuine and aware expectation to accessing and reaching thousands of digital contents and hundreds of online users that the data subject would either definitively want to reach (the "persons that you certainly wish to see" in the metaphorical invitation) or that he might have an interest to reach ("other people that you might want to know").

In a society where people living exclusively offline are social outcasts and people having limited access to online contents have less opportunities and are marginalized, a similar interest cannot be ignored.

It is a genuine and existential interest of people, most of the people actually, to have and live a life online - so-called onlife[59] - which is about finding and maintaining one's 'own place' in the digital dimension: to receive certain types of communication corresponding to certain types of interests and thus to access to thousands of online contents, selected among billions of online contents, and to stay in 'online touch' with hundreds of people and entities, selected among billions of online users.

An interest to receive personalised information amounts today to the interest to be included in, and to not be outcasted from, the dimension of digital communication and to have thus the possibility to have access to contents selected from billions of online contents. This amounts to say that there typically may be a very good reason to give a tied consent.

Being today tied consent an easy way to enter and remain into the digital environment, we shall also admit that the data subject's interest in giving a tied consent is per se worth of legal protection. Which amounts to reject the today's prevailing interpretation of article 7(4) GDPR according to which a tied consent would always be invalid for lack of freedom except in those limited (and frankly almost or statistically unrealistic) cases where real alternative services are offered without the payment of a price in money or the request of a tied consent.

The problem, rather, is that today tied consent not simply is an easy way to enter and remain in the digital environment, but it is the easiest way. And this is a problem, as it typically creates abuses and accidents. Data controllers are in a position to unfairly exploit the appetite of data subjects for personalised information and their interest to live online, and a number of typical accidents, harms (and even mental pathologies) are the consequence of certain types of interaction between humans and digital applications in particular in connection with the exposure to the outputs of AI systems.

In this light, therefore, the analysis needs to be complemented with that concerning the legal consideration of certain types of abuse and negative consequences attached to such phenomenon – the personalised communication – which implies to investigate the legal relevance of people's exposure to a number of risks in terms of manipulation, addiction and other mental illnesses, undesired contents, cyber risks, illicit or incorrect or unintended processing of own personal data; in all cases with the inherent analysis of the legal relevance of the causation of harm to data subjects and to third parties; as well as – when looking at the phenomenon of personalised communication in a broader perspective – the legal relevance of new issues of democratic and pluralistic guarantees intrinsic of the contemporary society, considering that the data driven economy implies a data industry and that data industry is a synonym for knowledge and culture industry.

At the same time - and this is the second next difficult assertion to demonstrate – the risks of most of the typical abuses and accidents attached to personalised communication are already contemplated and addressed by a number of mandatory provisions of Union law.

I make reference to:

[59] L Floridi, 'A look into the future impact of ICT on our lives' (2007) 23 Inf Soc, 61 ff.

- a number of mandatory provisions of contemporary data law that provide direct or indirect prohibitions on personal data processing; and
- the consequent need for a new interpretation of the GDPR's provisions relevant to privacy consent so as to recognize the invalidity of consent (article 6(1)(a) GDPR) and explicit consent (articles 9(2)(a) and 22(2)(c) GDPR) for reasons other than the lack of the requirements under art. 4(11) GDPR (including freedom), and specifically for unlawfulness of the processing's purposes for which the consent is given (article 5(1)(b) GDPR), which invalidity shall always be declared in the presence of processing activities that are in violation of any Union or national mandatory provisions laying down direct or indirect prohibitions on personal data processing.

4. The provisions of contemporary data law laying down direct or indirect prohibitions on personal data processing and the invalidity of privacy consent for illegitimacy of the processing purposes.

Data production is the character of the data-driven economy or data economy. Differently from what happened until some years ago in the 'information society', when information was essentially reproduced and communicated electronically, information is now also produced. Data are the result of manufacturing processes, whereby raw data[60] are processed and transformed in potentially infinite 'information refining processes' of an automatic nature. They bring about not only the risks of 'inference' relevant to inferred personal data to the detriment of individuals, as rightly highlighted by Cofone in The Privacy Fallacy[61], but also - more generally - a risk of failure of our society that I would call in terms of risk of crisis of 'artificial derivative knowledge', to a certain extent comparable to – but unfortunately infinitely more impacting than –the failure of the financial derivative instruments of some years ago.

In this scenario, it should be of no surprise to learn that legislators are laying down prohibitions and obligations to the data industry, designing limits to the private autonomy in this industry sector.

And, effectively, a number of sources of contemporary EU data law present mandatory provisions containing either direct or indirect prohibitions on the processing of certain data for certain purposes.

For the same reason, it is also necessary to consolidate the view that, as long as the interpretation and application of the GDPR is concerned, the processing of personal data shall pass a 'substantive' test of lawfulness aimed at assessing the observance or non-violation of mandatory provisions of Union and national law that directly or indirectly provide prohibitions on the processing of certain personal data for certain purposes. Such test shall be carried out in relation to any of the conditions or bases requested by the GDPR for the lawful processing of personal data.

[60] The expression 'raw data' is used in Recital 15 of the Data Act as well as in Chapter II of the European Commission's Guidelines '*Data Act explained*' of 22 April 2024.
[61] I Cofone, *The Privacy Fallacy* (1) 49-53, 74-76, 119-123, 165-172.

This actually is a *requirement* under the GDPR, although not a popular one. Article 5(1)(b) of the GDPR makes clear that personal data shall be collected and processed for «legitimate purposes». On this basis, it shall be recognized that this is an implicit legal requirement for each and all of the conditions for the lawful processing of personal data under article 6(1) GDPR. In particular:

- *(a)* consent by the data subject to the processing of her/his personal data for one or more specific purposes shall be read as necessarily referring to *legitimate* purposes;

- *(b)* performance of a contract shall necessarily be read as performance of a *legitimate* contract;

- each and all of the conditions sub letters *c)*, *d)* and *e)* of Article 6(1) GDPR – i.e. *(c)* compliance with a legal obligation, *(d)* protecting vital interests, and *(e)* performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – shall by definition read as referring to *legitimate* purposes and activities; and, finally

(f) legitimate interest shall be intended to refer to a lawful interest only, i.e. to necessarily imply legitimate purposes and activities.[62]

In this respect, it is worth remarking that, as said, a number of sources of contemporary EU data law present mandatory provisions containing either direct or indirect prohibitions on processing certain data for certain purposes. These sources are relevant for establishing whether or not the requirement of the legisyimate purpose under article 5(1)(b) GDPR is satisfied.

As regards direct prohibitions we can cite the directive on online platform workers,[63] the Digital Services Act (DSA),[64] the regulation on political advertising[65] and the EHDS regulation.

As regards indirect prohibitions, we can cite – to begin with - the regulation on artificial intelligence (AI Act),[66] but many other sources of EU and national law – as I will argue and demonstrate further in this paragraph and in the next paragraph – shall be included in this category.

Coming very briefly to each source: pursuant to Article 7 of the directive on online platform workers, digital labour platforms (as defined therein) are prohibited from processing by means of automated decision-making or monitoring systems (as defined therein): (a) personal data relating to the emotional or psychological state of the person performing platform work; (b) personal data relating to private conversations; (c) personal data where the person performing platform work is not performing platform work or is not offering to do so; (d) personal data to provide for the exercise of fundamental rights, including the right of association, the right to collective bargaining and

[62] See ECJ, Judgment of the Court (Ninth Chamber) of 4 October 2024, case C-621/22 EU:C:2024:858, point 40.

[63] Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work. [2024], L 11/11/2024

[64] 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)., [2022], OJ L 277/1

[65] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] , OJ L 20/03/2024

[66] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), [2024] OJ L 12/07/2024

collective action, or the right to information and consultation, as defined in the Charter of Fundamental Rights of the European Union; (e) personal data to infer a person's racial or ethnic origin, migrant status, political opinions, religious or philosophical beliefs, disability, state of health, including chronic diseases or HIV status, emotional or psychological state, membership of a trade union, sex life or sexual orientation; (f) biometric data, as defined in the GDPR, of a person performing platform work to establish his or her identity by comparing it with the biometric data of persons stored in a database.

Prohibitions on processing certain personal data (those under Article 9(1) GDPR) for certain marketing purposes are disposed by both the DSA[67] and the regulation on political advertising,[68] and the DSA also contains a similar prohibition on processing personal data of minors.[69]

Finally, the EHDS regulation contains a number of prohibitions on certain secondary uses of health electronic data.[70]

With 'indirect prohibitions', I make reference to those mandatory rules that do not directly prohibit certain processing activities, but that prohibit certain other activities which necessarily and typically presuppose certain data-processing activities.

The most evident example is that of the prohibitions contained in Article 5 of the AI Act on the placing on the market, putting into service and use of certain AI systems. Any processing of personal data for the development and

[67] Art. 26(3) DSA provides that providers of online platforms may not present advertisements to service recipients based on profiling (as defined in the GDPR) using the special categories of personal data set out in Article 9(1) GDPR.

[68] Article 18(1)(c) of Regulation (EU) 2024/900 on the transparency and targeting of political advertising prohibits targeting or delivery techniques in the context of online political advertising that make use of profiling techniques (as defined in the GDPR) using the special categories of personal data set out in Article 9(1) GDPR.

[69] Art. 28(2) DSA prohibits online platform providers from presenting profiling-based advertising (as defined in the GDPR) using the personal data of the service recipient on their interface if they are aware, with reasonable certainty, that the service recipient is a minor.

[70] Article 54 of the EHDS regulation: "Health data users shall only process electronic health data for secondary use on the basis of and in accordance with the purposes contained in a data permit issued pursuant to Article 68, health data requests approved pursuant to Article 69 or, in situations referred to in Article 67(3), an access approval from the relevant authorised participant in HealthData@EU referred to in Article 75.

In particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 68 or a health data request approved pursuant to Article 69 for the following uses shall be prohibited:

(a)taking decisions detrimental to a natural person or a group of natural persons based on their electronic health data; in order to qualify as 'decisions' for the purposes of this point, they have to produce legal, social or economic effects or similarly significantly affect those natural persons;

(b)taking decisions in relation to a natural person or a group of natural persons in relation to job offers, offering less favourable terms in the provision of goods or services, including exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or conditions of loans, or taking any other decisions in relation to a natural person or a group of natural persons which result in discriminating against them on the basis of the health data obtained;

(c) carrying out advertising or marketing activities;

(d) developing products or services that may harm individuals, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction, contravene public order or cause a risk for human health;

(e) carrying out activities in conflict with ethical provisions laid down in national law".

use of those systems shall be deemed carried out for an illegitimate purpose, thus qualifying as an unlawful processing pursuant to the GDPR.

But there is no reason to limit the analysis to the provisions of the AI Act, because there are automated processing of personal data, including automated processing of personal data carried out by AI systems, which can be considered unlawful on the basis of other mandatory provisions.

We can think, for example, of online platforms that process personal data for games of chance or prize competitions in violation of mandatory provisions of national laws governing these activities.

Even in such cases the related processing of personal data will have to be considered unlawful under the GDPR (including, of course, in cases in which the platforms in question make use of artificial intelligence systems).

And in fact, in similar cases we would certainly be in the presence of a violation of the principle expressed by Article 5(1)(b) GDPR according to which personal data must be collected for legitimate purposes.

In all these cases, any data subject's consent (pursuant to Art. 6(1) GDPR) or explicit consent (pursuant to Articles 9(2) or 22(2)(c) GDPR), would be invalid as it would be given for a processing activity that pursues illegitimate purposes.

5. The invalidity of Mr. Leon's consent to the processing of his personal data for the purpose of making him the target of an aggressive commercial practice.

The same conclusion - as to the invalidity of the privacy consent for illegitimacy of the processing purpose – shall be drawn with respect to the violation of the mandatory provisions of the UCPD, whenever the commercial practice in question implies the processing of personal data. In that case, as explained in general terms in paragraph 4 above, we are in the presence of a violation of a mandatory provision laying down an indirect prohibition on personal data processing. In fact, as explained in paragraph 4 above, the principle stated in article 5(1)(b) GDPR that personal data shall be collected and processed for legitimate purposes certainly contains a prohibition on collecting and processing personal data for illegitimate purposes, and the processing carried out for putting in place activities that are prohibited by mandatory provisions - such as unfair commercial practices pursuant to the UCPD - certainly entails the case of a data processing activity carried out for an illegitimate purpose, i.e. an unlawful processing.

To demonstrate how important and far-reaching this perspective is, I will use two examples contained in the already quoted EDPB Guidelines 8/2020 on the targeting of social media users (the EDPB Guidelines 8/2020 or the Guidelines).

Example 7 of EDPB Guidelines 8/2020 regards Mrs Delucca, a person interested in impressionist paintings.[71] In this example, Mrs Delucca, after having posted many times her "likes" to photos of paintings by an impressionist painter posted by an art gallery, receives on her social media page a targeted advertisement related to an upcoming exhibition of impressionist paintings made by a museum, that, in order to attract visitors, had used the following

[71] EDPB Guidelines 8/2020, point 80, p. 24.

targeting criteria offered by the social media provider: "interested in impressionism", gender, age and place of residence.

In this case, it is easy to see how Mrs Delucca has a genuine interest in receiving this kind of information, as it gives her the possibility to visit an exhibition of paintings in line with her artistic tastes, plus the potential to learn about new works and new artists, as well as to get in touch with individuals/organizations/entities that have the same interests or tastes as her or are professionally active in the field of impressionist paintings. Without a profiling and targeting based on the processing of her personal data, Mrs Delucca would likely have not come across that exhibition and certainly would not have learnt about it so rapidly and without the need to employ her time to carry out searches about forthcoming exhibitions. This example demonstrates that an interest of the data subject may well exist behind personalised information, and that it is an interest worth of legal protection. This example illustrates and confirm that in similar cases a tied consent may pursue interests that are worth of legal protection, considering the interests of all the subjects involved in the personal data processing (see paragraph 3 above).

Example 8 of the EDPB Guidelines 8/2020 reads as follows: «Mr Leon has indicated on his social media page that he is interested in sports […]. He also visits a number of online gambling websites. The social media provider tracks Mr Leon' online activity across his multiple devices […] In addition, the social media platform has developed targeting criteria enabling companies to target people who are likely to be impulsive and have a lower income. The online betting company "bestpaydayloans" wishes to target users that are interested in betting and that are likely to be betting heavily. It therefore selects the criteria offered by the social media provider to target the audience to whom its advertisement should be displayed».[72]

The profiling activity carried out in this example (Mr Leon) may appear similar to that of the preceding example (Mrs Delucca), while it presents a very significant difference in legal terms, and as a matter of Union law in particular. In fact, in the case of the example of Mrs Delucca, the profiling activity is carried out on the basis of criteria and for a specific targeting purpose – revolving around the interest for impressionist paintings – that do not denote a situation of vulnerability, and is designed to the sending of personalised advertising to the benefit of the data subject (who, in the case under the example, learns about an exhibition of interest to her). On the contrary, the example of Mr Leon shows a profiling activity based on targeting criteria – such as 'impulsive character' and 'lower income' – that are used for identifying individuals specifically vulnerable to certain advertising messages. In particular, under Example 8 the social media platform has developed targeting criteria enabling companies to target people that are likely to be impulsive and have a low income, whose behaviour can be typically distorted precisely because of the combination and coexistence of those specific two (character- and income-related) features. This example denotes the creation of a target through vulnerabilities, namely a consumer target which, precisely because of those two personal data-features processed by an algorithm (impulsivity and low

[72] EDPB Guidelines 8/2020, point 80, pp. 24-25.

income), typically presents by inference a lack of capacity to resist to a certain commercial practice (online betting advertising). This certainly amounts to an unfair commercial practice, more precisely an aggressive commercial practice, under the UCPD (see paragraph 2 above).

Therefore, while in the first case the interest of Mrs Delucca to be profiled and to receive that type of information is worth of protection, in the second case it cannot be admitted that Mr Leon is made subject – not even with his explicit consent – to a similar aggressive commercial practice, which is precisely designed to exploit specific and well known decisional and behavioural vulnerabilities of the targeted person, who is identified and treated as the target of that advertising exactly because of those vulnerabilities (see also paragraph 2 above).

However, this is today admitted by the EDPB. In fact, in the same EDPB Guidelines 8/2020, and in connection with Example 8, it is written that Mr Leon through his explicit consent pursuant to article 22 GDPR may validly authorize the processing of his personal data for the purpose of making him the target of that online betting advertising, i.e. a commercial practice precisely designed for exploiting a behavioural vulnerability of Mr Leon.[73]

In this respect, it appears worth reminding the EDPB-EDPS Joint Opinion 5/2021 of 18 June 2021 on the AI Act's proposal [74] (the Joint Opinion).

The Joint Opinion - contemporary with the EDPB Guidelines 8/2020 [75]- is a very important opinion. I will confine myself to recall the part of the Joint Opinion dedicated to the AI emotion recognition systems, in order to compare the relevant comments with the discussion of Example 8 under the Guidelines.

Point 35 of the Joint Opinion reads as follows: «[…] the EDPB and the EDPS consider that the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited, except for certain well specified use-cases, namely for health or research purposes (e.g., patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation».

This position is clearly inconsistent with the interpretation of the explicit consent under article 22 GDPR, contained in the Guidelines, according to which explicit consent would constitute a valid legal basis for processing personal data for the specific purpose of exploiting impulsivity. As argued in this paragraph and in paragraph 4 above, this is a wrong interpretation of article 22 GDPR as it is in contrast with the principle of article 5(1)(b) GDPR that

[73] EDPB Guidelines 8/2020, pp. 25-26, points 82, 85, 86, 87 and 88: «In such circumstances as described in Example 8, the display of online betting advertisements may fall under the scope of Article 22 GDPR (targeting financially vulnerable persons that are interested in online betting which have the potential to significantly and adversely affect his financial situation). Therefore, in accordance with Article 22, explicit consent would be required. Furthermore, the use of tracking techniques triggers the applicability of Article 5(3) of the ePrivacy Directive, resulting in a requirement of prior consent. Finally, the EDPB recalls that for the processing to be lawful, the controller must conduct a case-by-case assessment, and that obtaining consent does not reduce other obligations to observe the requirements of fairness, necessity, proportionality and data quality, as stated in Article 5 GDPR».

[74] EDPB-European Data Protection Supervisor (EDPS) Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) of 18 June 2021.

[75] Version 2.0 of the Guidelines was adopted on 13 April 2021.

prescribes that personal data shall be collected and processed for legitimate purposes.

Rather, examples 7 and 8 of the Guidelines indicate the need to recognize that the most common formulas used in the online market to express the stated purpose of the personal data processing (i.e. the formulas on the basis of which privacy consent is ordinarily requested and given) such as “profiling” “marketing” “targeting” “advertising” are not sufficient to conclude on the lawfulness of the processing purpose, and, thus, on the validity of the privacy consent, simply because – as already argued in general terms in paragraph 2 above – marketing can be either fair or unfair depending on how marketing practices are designed in practice.

As demonstrated by the two examples of Mrs Delucca and Mr Leon, targeting algorithms are designed and work for stated purposes. It is therefore necessary to analyse in detail the targeting algorithms to establish on a case-by-case basis the legitimacy of the processing purposes. And it is necessary to distinguish between those algorithms pursuing legitimate purposes and those pursuing illegitimate purposes, since – as acknowledged by the EDPB trough the example of Mr Leon – algorithms designed precisely for exploiting behavioural and decisional vulnerabilities of online users do exist and are widespread in the online market.

As regards the validity of privacy consent, I am not talking here about the requirement of specificity or ‘granularity’ of the privacy consent. If Mr Leon – to use the example elaborated by the EDPB – gave an explicit consent specifically to the functioning of an algorithm collecting and processing his personal data relevant to his impulsivity and his income, still any such explicit specific and granular consent would be invalid pursuant to article 5(1)(b) GDPR.

Rather, I am talking about the need to advocate an interpretation of privacy consent that is capable to conclude for the total invalidity or - as the case may be - the partial invalidity of the consent depending on the legitimacy and the extent of the processing purpose(s). Much like it happens in the field of consumer contracts since directive 93/13/EEC (the rationale of whose rule that unfair contract terms are not binding while the contract remains binding without the unfair terms is that consumers are not in a position to fruitfully examine and negotiate all the contract terms and should not be required to do so) it is opportune to recognize that data subjects are not in a position to fruitfully examine and negotiate any of the targeting and marketing algorithms and they shall not be required to do so, with the consequence that any privacy consent, including any tied consent and explicit consent, shall be totally or partially valid/invalid to the extent the stated processing purpose(s) is/are in practice legitimate/illegitimate pursuant to article 5(1)(b) GDPR.

6. Relational nature of data.

It is also opportune to note – following up with the example of Mr Leon discussed in paragraph 5 above – that the interests at stake here are not simply those relevant to Mr Leon, and not even more generally those regarding the fundamental rights of Mr Leon, as the invalidity of Mr Leon’s privacy consent is

aimed at protecting a collective interest: the community does not want that no one's personal data are being processed to exploit and to take advantage of conditions of behavioural and decisional vulnerability; including conditions of vulnerability of persons other than the data subject whose personal data are being processed.

If Mr X is *not* an impulsive person and his personal data (online behaviour), together with those of many other not impulsive and impulsive people are collected and processed for developing an AI system that exploits impulsivity, the processing of Mr X's personal data too is unlawful, and any consent given by Mr X for the development of any such AI system would be invalid, in the sense illustrated above (paragraph 5 above).

The same would apply of course with respect to the personal data of an impulsive person having regard to the collective interest to not train manipulative systems exploiting the impulsivity of third parties.

Even if any such personal data were immediately and definitively anonymised, it would not make any difference: article 5(1)(b) GDPR does not admit (and it is a collective interest of the community to not admit) that personal data are used for developing and training AI systems that distort people's behaviour, because this is an illegitimate purpose.

It is therefore very appropriate that Ignacio Cofone in his book captured and commented on the relational nature of personal data.[76] In brief, it shall be recognised that, in the AI environment, the processing of personal data has a potential to be harmful not only to the relevant data subjects but also to third parties, or even only to third parties.

7. Characters of new EU data law.

The 'new' EU data law, as resulting from the strategy-documents of the EU institutions,[77] and, more importantly, from EU directives and regulations recently adopted,[78] presents a series of stable features, in summary:

1) the digital dimension, for which the 'data' relevant for the new disciplines of Union law only are electronic data;[79]

2) a new paradigm of protection of the data subject, based, rather than on his privacy consent and opt-out, on:

(i) the typification of legitimate and illegitimate processing purposes, which brings about, *inter alia*, the important issue (discussed in this paper) of the invalidity of the privacy consent for the illegitimacy of the processing purposes;

[76] See also the very interesting essay of 2021 by Salomé Viljoen: S Viljoen, 'Democratic Data: A Relational Theory For Data Governance'(2021)131, Yale L J 370 ff.

[77] See in particular: the "*International Digital Strategy for the European Union"* of 5 June 2025 adopted by the European Commission and the High Representative for Foreign Affairs and Security Policy; the European Commission's Communication COM(2025) 165 final of 9 April 2025 "*The AI Continent Action Plan*; the European Commission's Communication (COM(2020) 66 final of 19 February 2020 "*European Strategy for Data*".

[78] I make reference to the many sources of Union law quoted in paragraphs from 2 to 6 above.

[79] See: art. 2, n. 1 Data Governance Act; art. 2, n. 24 Digital Markets Act; art. 2, n. 1 Data Act; art. 2(1)(c) and art. 2(2)(a), (b) and (c) reg. EHDS.

(ii) new forms of data sharing, including restricted access to data in secure processing environments;[80] and

(iii) security of the infrastructures through which the data sharing is realized in the forms prescribed by the law;

3) a new paradigm for non-personal data governance, whose sharing within the Union market is promoted, while at the same time new significant restrictions are put in place for the transfer to and access from countries outside the Union market, comparable to those traditionally provided for personal data.[81]

Coming to the only feature of relevance in our discussion, and as extensively highlighted in paragraph 4 above, many mandatory provisions of Union law (as well as a number of sources of national law in the various Member States[82]) present the character sub 2*(i)* above.

As a consequence of this feature, the following two important issues (among others) need to be addressed in contemporary EU data law: *(i)* the procurement by the competent authorities of sufficient and adequate technological resources for carrying out the necessary analyses on the automated processing of electronic data at an algorithm-level; and *(ii)* the coordination, for enforcement purposes, among the various authorities that are competent in the fields of activity interested by the data processing, taking into consideration the competences of the data protection authorities (on one side) and the competences of the other administrative and/or judiciary authorities that are vested with the powers to enforce the mandatory provisions prohibiting those activities that imply the personal data processing in the various fields of law (on the other side).

8. Conclusive remarks.

In the present notes I have not at all intended to deny the need to make the most of the remedies available in tort, and to elaborate around damages compensation – which is the perspective highlighted and supported by Ignacio Cofone in *The Privacy Fallacy* – while I have intended to suggest (as done in previous papers) a fairly new interpretation of the provisions of the GDPR relevant to privacy consent taking into account certain features of EU data law as emerging from a number of recent EU regulations, and some important principles of EU consumer law, as recently evolved into 'online user law'.

As to the last point, I have highlighted in this paper the need to consider the solid set of mandatory provisions of Union law that have the purpose of countering behavioural distortion and that *already* take into account the results

[80] See art. 2, n. 20 Data Governance Act; art. 2(1)(c) reg. EHDS.

[81] See art. 89 reg. EHDS; art. 31 Data Governance Act; art. 32 Data Act.

[82] This is the case, for instance, of the laws on the so-called 'oncological oblivion' enacted in some countries in line with the recommendation contained in point 125 of the European Parliament resolution of 16 February 2022 on strengthening Europe in the fight against cancer (P9_TA(2022)0038), containing prohibitions on collecting and processing personal data relative to 'cancer survivors' for purposes unrelated to health assistance, intended to avoid discrimination against cancer survivors in contractual relationships as well as in other relationships specifically considered by the various laws. See S Orlando, 'Oncological oblivion', in *Digitalization in Health Care between New Technologies, Data and Research* by A. Bernes (ed.), Springer, forthcoming.

of behavioural economics and neurosciences, in the part they protect *free* (as opposite to informed) decisions of consumers and online users at large.[83]

As regards EU data law, as said, it should be acknowledged, on one side, the reduced role of the privacy consent and of the data subject's opt-out in recent EU legislation, the rise of cases where the sharing of personal data is believed to be of a collective interest, as well as the increasing number of mandatory provisions laying down direct and indirect prohibitions on personal data processing, which is an entirely sensible novelty explainable with the awareness of the characters of the 'data-driven society', where information is massively produced by way of processing other information, and not only reproduced and transmitted electronically, as it happened until some years ago in the 'information society'.[84]

In order to put the new provisions of EU data law in (historical) context, it is also necessary to realize that the sharing of personal data in the online environment is an inevitable phenomenon and not one to counter *as such*, because, as noted, people have an interest worth of legal protection to be and act as online users and to access to personalised information.[85] Neither it is a phenomenon that can be left to the full discretion or authorization of the data subject, since, on one side, there is a growing awareness of the existence of a collective interest to make certain personal data available for purposes that are beneficial to the community,[86] and, on the other side, it shall be recognized that it is an interest of the community (a collective interest), not only an individual interest of the data subject, to ensure that the processing of anyone's personal data does not pursue illegitimate purposes: both purposes that are detrimental to the data subject[87] and purposes that can be detrimental to persons other than the data subject.[88]

In short, much as it happens for the offline life, also with respect to the activities consisting in the processing of electronic personal data in the online environment it is correct to observe that the law supports activities that are (believed to be) beneficial to the community and counter activities that are (believed to be) harmful. Damages compensation is certainly part of the deterrence measures aimed at countering harmful activities, but many other measures exist as a matter of Union law which are implied with the enforcement of mandatory provisions laying down direct or indirect prohibitions on data processing; and they should be better evidenced and effectively adopted, especially public enforcement measures in the forms of banning orders and fines.

Coming to the GDPR, I believe that a hermeneutic way exists for both factoring in in the analysis relevant to the privacy consent the historical context of the online dimension where personal data are collected and produced (inferred), and avoiding at the same time the risks, opportunely indicated by Cofone, associated with the common interpretation of the Regulation,

[83] See para. 2 and 5 above.
[84] See para. 4 and 7 above.
[85] See para. 3 and 5 above.
[86] See para. 7 above.
[87] See para. 4 and 5 above.
[88] See para 6 above.

resulting in limiting controller's accountability to procedural compliance and to procedural adherence to privacy policies.

For the reasons that I have tried to summarise in the present contribution[89] (and expanded in previous articles in Italian language)[90], I believe that the GDPR can and should be interpreted so as to recognize that a substantive test of validity of the privacy consent is required based on the legitimacy of the processing purposes pursuant to the imperative principle of article 5(1)(b) GDPR, with the consequence that any privacy consent (including any tied and explicit consent) should be considered ineffective in all cases in which the data processing is either directly prohibited by a mandatory provision of Union or national law or it is necessary for realizing an activity which is prohibited by a mandatory provision of Union or national law.

Accountability of the controller would then cease to be interpreted in a procedural fashion - as comprehensibly criticised by Ignacio Cofone[91] - *pari passu* with the bureaucratic reading of all the conditions under article 6(1) GDPR.

In the end, if the provisions of articles 5(2) [92] and 5(1)(b) GDPR were correctly interpreted in combination one with the other, it would certainly be possible to conclude – to use Ignacio's words - that also for the GDPR controller's responsibility means accountability for the use or misuse of people's personal data.[93]

I am conscious that this is a new reading of the GDPR, but I also believe that the traditionalist interpretation of privacy consent, which does not question the legitimacy of the processing purpose, is wrong for being it in contrast with article 5(1)(b) GDPR nor is it adequate for the times in which we live.

Ignacio is certainly right to observe that privacy law needs an update,[94] and many authors have noted that the GDPR is already obsolete. Law reforms are always possible, and in the old continent they are constantly in sight as we keep on reading and interpreting.

[89] See para. 4 and 5 above.

[90] S Orlando, 'Consenso al trattamento e liceità' (2024) 2 Persona e Mercato 33 ff; S Orlando, 'Sulla necessita` di un controllo di liceita` sostanziale per tutte le basi del trattamento dei dati personali'(2024)3 Persona e Mercato 815 ff

[91] I Cofone, *The Privacy Fallacy*, (1) 170.

[92] Article 5(2) GDPR: «The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')»

[93] I Cofone, *The Privacy Fallacy*, (1) 170: «Because of the information economy's moral hazard, "responsibility" must mean accountability for the outcomes of how corporations use (or misuse) people's personal data».

[94] I Cofone, *The Privacy Fallacy*, (1) 165.