1

Net Neutrality matters: Privacy antibodies for information monopolies and mass profiling

Gianluigi M. Riva
University College Dublin, School of Information and Communications Studies, Dublin, Ireland. E-mail: gianluigi.riva@ucd.ie

Marguerite Barry
University College Dublin, School of Information and Communications Studies, Dublin, Ireland. E-mail: marguerite.barry@ucd.ie

Abstract
Profiling activities used to personalise user content can place online corporations in a position of significant influence over user behaviour. The ability to deliver different search engine results, news feeds, discriminatory prices, and so forth, can be exploited to grant unequal access to different kinds of content. This is likely to intensify with the Internet of Things (IoT), which will surround individuals with sensors capable of 24/7 full tracking. This content-shaping power jeopardises the neutral accessibility that a democratic internet should ensure. Indeed, both neutrality and accessibility should refer not only to the service connection but also to the content it delivers. This study examines this personalisation and filtering power in light of Privacy and Data Protection regulations to explore how privacy principles can be used to enhance IoT accessibility. It elaborates a comparative analysis of legislative sources related to public goods and interests, data flows and contract law relationships, into a holistic narrative reasoning. The discussion addresses the monopolistic economic position of platforms, their connected revenue models and the power to control and influence information. Fake news plays a crucial role in this and is addressed consequently. Therefore, the study analyses how these factors together could form profiling 'multi-monopolies' in connection with a non-neutral Internet of Things. Furthermore, techniques of influence have more grip where there is a lack of awareness and knowledge, and a new model of digital "*divide et impera*" seems to enhance these phenomena. Besides, social score systems and discriminatory pricing can be powerful tools in this sense. We discuss the gap between regulatory approaches and real-world situations, offering common legal tools and Privacy by Design (PbD) as potential solutions for neutral accessibility. We highlight how the current regulatory framework requires more harmonisation to guarantee effective user protections, especially in an IoT ecosystem.

Keywords

Revista Publicum
Rio de Janeiro, v. 5, n. 2, p. 7-35, 2019
http://www.e-publicacoes.uerj.br/index.php/publicum
DOI: 10.12957/publicum.2019.47199

Privacy by Design; Profiling; Net Neutrality; Fake news; Discriminatory pricing; Social credit system; IoT.

Neutralidade da rede importa: anticorpos de privacidade para monopólios de informação e profiling *em massa*

Resumo

As atividades de *profiling* usadas para personalizar o conteúdo disponibilizado aos usuários podem colocar as empresas de Internet em uma posição de influência significativa sobre o seu comportamento. A capacidade de fornecer diferentes resultados de mecanismos de pesquisa, *feeds* de notícias, preços discriminatórios, dentre outras, pode ser explorada para garantir acesso desigual a diferentes tipos de conteúdo. É provável que isso se intensifique com a Internet das Coisas (IoT), que cercará indivíduos com sensores capazes de rastreamento completo 24 horas por dia, 7 dias por semana. Esse poder de modelagem de conteúdo põe em risco a acessibilidade neutra que uma Internet democrática deve garantir. De fato, tanto a neutralidade quanto a acessibilidade devem se referir não apenas à conexão do serviço, mas também ao conteúdo que ele fornece. Este estudo examina esse poder de personalização e filtragem à luz dos regulamentos de Privacidade e Proteção de Dados para explorar como os princípios de privacidade podem ser usados para aprimorar a acessibilidade da IoT. Elabora-se uma análise comparativa de fontes legislativas relacionadas a bens e interesses públicos, fluxos de dados e relações de direito contratual, em um raciocínio narrativo holístico. A discussão aborda a posição econômica monopolista das plataformas, seus modelos conectados de receita e o poder de controlar e influenciar as informações. *Fake news* desempenham um papel crucial nisso e, consequentemente, são abordadas. Portanto, o estudo analisa como esses fatores podem, juntos, formar 'multimonopólios' de *profiling* em conexão com uma Internet das Coisas não neutra. Além disso, as técnicas de influência são mais abrangentes onde há falta de consciência e conhecimento, e um novo modelo digital de “dividir para conquistar” parece intensificar esses fenômenos. Ademais, sistemas de pontuação social e preços discriminatórios podem ser ferramentas poderosas nesse sentido. Discutimos a lacuna entre abordagens regulatórias e situações do mundo real, oferecendo ferramentas legais comuns e o *Privacy by Design* (PbD) como possíveis soluções para acessibilidade neutra. Destacamos como a atual estrutura regulatória exige mais harmonização para garantir proteções efetivas ao usuário, especialmente em um ecossistema de IoT.

Palavras-chave

Privacy by design; Profiling; Neutralidade da rede; Fake news; Preços discriminatórios; Sistema de crédito social; Internet das Coisas.

Table of Contents | Sumário

Multi-monopolists; 3.2 How disinformation creates uncertainty and how both are tools of control; 3.3 Zero-rating and social credit scoring; 3.4 Mass customization through pricing personalization and discrimination; 4. Neutral accessibility and privacy by design solutions; 4.1 The right to access content as a form of ingress-egress over a digital easement; 4.2 Data accessibility and 'Neutrality by Design'; 4.3 Regulatory harmonization; 4.4 Privacy by Design with user-in-control solutions; 5. Conclusion; References; Acknowledgements.

1. Introduction

The Internet is a powerful tool and, as with every technology in history, its threats are proportional to its utility. Yet, nowadays, the Internet is to the Internet of Things as the telegraph was to telephone. The IoT will soon disrupt how we think about communication and is likely to enhance Internet companies' power exponentially, for better or worse. Net Neutrality is a central concept in this regard and the legal regime governing it in Europe and (recently abandoned[1]) in the US, has broad implications for information management and production. In general, "neutrality" is the tendency to maintain an attitude of impartiality toward all parties[2]. Net Neutrality is the principle according to which Internet service providers (ISPs) must treat all Internet communications equally, and not discriminate or charge differently based on user, content, website, platform, application, type of equipment, source address, destination address, or method of communication[3].Therefore, with 'neutrality' of technologies, services and regulation, we refer to a general principle of non-discrimination as the right of accessibility for everyone at the same conditions[4].

This study evaluates these implications in light of Privacy and Data Protection regulations, which currently find the highest worldwide standards in the EU General Data Protection Regulation[5] (GDPR). This work highlights the risks posed for society with the advance of IoT systems into our daily reality, without the support of adequately updated legal rules to govern them. It reveals the intricate connection between profiling[6], 'mass customisation'[7], social score

[1] On June 2018 the American FTC voted to repeal the 2015 Open Internet Order (on Net Neutrality principle) came into effect.
[2] https://www.britannica.com/topic/neutrality (last visited November 7, 2019).
[3] https://www.wired.com/story/guide-net-neutrality/(last visited November 7, 2019).
[4] Mercedes Fuertes, *Endefensa de la neutralidad de la red*, 99:100 R.V.A.P., 1397-1412 (2014).
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
[6] The concept will be explained specifically in the following § 2.1.
[7] This concept that we propose will be explained in the following § 1.1.

systems[8], fake news[9], as well as mis-[10] and dis-[11]information that, when interconnected, create an ecosystem with prevailing economic and legal questions of global scope. This contribution outlines the cause and effect relationship between various components of this economic-technological system and proposes practical legal solutions based on the application of the current (fragmented) European regulatory framework. The study aims to create a big-picture overview of interconnected phenomena that the existing literature addresses individually in separate domains. It proposes an argumentative bridge between these components to present a holistic study of a general and complex phenomenon, addressed through the technological and legal lenses of profiling and information control, in their various articulations.

The paper first provides a general overview of the critical concepts that interconnect the topic. It then addresses specifically the profiling activities and their relationship with the Net Neutrality and the economy of the Internet. It moves head in analysing the relevant legal aspects of the phenomenon, and how discriminatory pricing and data scoring impact on the users-ISPs relationship. The paper then focuses on the multi-monopoly phenomenon and how it relates to Data Protection and Consumer Law. Through these lenses, it performs a specific analysis of zero-rating techniques and the role of social credit scoring systems in light of mass customisation. The work then affords the concept of Net accessibility with a comparative analysis of offline legal regimes and provides insights for harmonising the regulatory framework and building Privacy by Design solutions around it. It finally concludes the analysis highlighting the crucial role of both the Law and education, in order to grant effective participation in a 'Neutrality by Design' democratic process.

1.1 Background

When the Net lacks neutrality, ISPs and platforms are in the position of arbitrarily deciding who can access what content under what conditions (e.g. broadcasting speed). This offers enormous

[8] A.k.a. as Social Credit System, i.e. the activity of scoring human behaviour with a reputational system (which in China is made public in those area in which is experimented) based on the adherence to legal provisions or social norms and functioning thanks to digital surveillance systems.https://en.wikipedia.org/wiki/Social_Credit_System(last visited November 7, 2019).

[9] Fake news is often defined as a form of journalism which consists of deliberate disinformation or hoaxes spread via traditional news media (print and broadcast) or online social media.https://en.wikipedia.org/wiki/Fake_news(last visited November 7, 2019).

[10] Misinformation is false or inaccurate information. Examples of misinformation include false rumours, insults and pranks, while examples of more deliberate disinformation include malicious content such as hoaxes, spear phishing and computational propaganda.https://en.wikipedia.org/wiki/Misinformation(last visited November 7, 2019).

[11] Disinformation is false information spread deliberately to deceive. This is a subset of misinformation, which also may be unintentional. The English word disinformation is a loan translation of the Russian dezinformatsiya, derived from the title of a KGB black propaganda department.https://en.wikipedia.org/wiki/Disinformation

political and commercial power based on the interrelation between revenue models and profiling activities through data mining. This power can be described as 'mass customisation', which allows for the governance of users' activities by contemporaneously managing mass flows and individuals' relationships between each other as well as among platforms. Fake news and misinformation are also powerful tools in this regard and can be read through the lenses of mass influence[12], amplified by invasive profiling and political-economic power, as determined by dominant positions of 'multi-monopolies'[13]. Therefore, profilingand its relationship to disinformation and misinformation is a growing challenge for the information society where control over the chain of information production, validation, management and supply grants platforms a significant and potentially manipulative power.

These dynamic and interrelated phenomena are immersed in the information economy, together with infrastructure, regulatory frameworks and our social relationships. Themanagement of information (and disinformation) and the potential abuse of this power in economic terms can be viewed as a 'profile and rule'strategy, i.e.a modern version of *divide et impera*[14]. Where the legal landscape is fragmented and uneven in dealing harmoniously with such scenarios, individuals are left isolated in addressing this disproportionate power. User protection can be enhanced, however, by the general principle of democratisation, considered as a collective interest and fundamental right in both participation and access. Internet democratisation involves two aspects: democratic access and democratic participation, concepts which need to be understood considering what democracy conveys in terms of collective consensus. Participation is a core element in democracy but cannot be a standalone concept without connection to other essential elements, such as equality and autonomy, among others. In turn, autonomy is the cornerstone of democracy as a form of the collective decision-making process[15], which is crystallised in an individuals' consent. Autonomy is the fundamental element that renders decisions free and, therefore, is an essential and necessary prerequisite to self-determination. This is the first parallelism with Privacy because a data subject's consent must also be free[16], which legally implies that it is specific, informed and unambiguous. Where

[12] Hunt Alcott & Matthew Genztkow, *Social Media and Fake News in the 2016 Election,* 31:2 J. of Economic Perspectives, 211–236 (2017).
[13] N. Kulathuramaiyer& W.T. Blake, *Restricting the View and Connecting the Dots - Dangers of a Web Search Engine Monopoly*, 12:12 J. of Universal Comp. Sc., 1731-1740 (2006).
[14] https://en.wikipedia.org/wiki/Divide_and_rule (last visited September 30, 2019).
[15] Deborah G. Johnson, *Democracy, Technology, and Information Societies*, in: Philippe Goujon et al. (eds.), *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleurs.j*., 233 IFIP International Federation for Information Processing, Springer, Boston, MA, (2017).
[16] GDPR Article 4(1) n. 11)

"informed consent"[17] is not really informed, or where consent is in some way manipulated, the decision-making process is not free, and so is neither valid nor lawful.

Information itself embraces the concept of accessibility, as access to knowledge is the only way to reach a sufficient level of understanding to take an autonomous decision. Understanding information is a further step, as people must comprehend what they access. The sum of autonomous informed and educated participation represents thedemocratic consensus. However, consensus itself can also be influenced (meaning every hetero-determined external activity that deprives autonomy), and this is the common thread that connects what we can call the 'Net (of Things) Neutrality' to the Data Protection realm, specifically regarding profiling activities and information control.

In general, the broad approach to democracy and technology is far from univocal, and there is debate among scholars about whether technology enhances democracy or not. For example, Odifreddi (2011) maintains that democracy is mathematically impossible[18], while Rampini (2015) argues that the utopia of the Internet as a free-land in which everybody could have granted their own space, was a sort of "hippie" illusion that, indeed, has been completely reversed by the capitalistic model of disintermediation[19],[20]. However, some support the idea of avoiding the mistake of assuming the technology as something deterministic, merely physical (objects and artefacts) and neutral[21]. In fact, the technological state of the art is the result of a process in which many factors concur and, conversely, society is not the deterministic product of technological applications[22]. Indeed, social, cultural and many other variables intervene in these dynamic processes. The Internet is an excellent example of the misunderstood conceptualisation of technology as a material thing because, in technological terms, the net is far more than the sole sum of its material elements (hardware, software, cables)[23]. On the other hand, technology also crystallises certain values, biases, needs, and limits, (not to mentionforms of knowledge)[24], which shape its ultimate features[25]. Indeed, the current Internet architecture tends to support a centralising power strategy andcan be connected to the economic need to support centralised

[17] GDPR Article 13 and 14.
[18] Pier Giorgio Odifreddi, *La democrazia impossibile*, in: Ciro Ciliberto & Roberto Lucchetti (eds.), *Un mondo di idee*, I blu (pagine di scienza), Springer, Milano, (2011).
[19] Federico Rampini, *Rete padrona. Amazon, Apple, Google & co. Il volto oscuro della rivoluzione digitale*, Feltrinelli, (2015).
[20] See also Howard Rheingold, *The Virtual Community. Homesteading on the Electronic Frontier*, Reading: Addison-Wesley, (1993).
[21] D.G. Johnson, *ibid.*
[22] Wiebe E. Bijker, *How is technology made?—That is the question!*, 34:1 Cambridge J.of Economics, 63-76 (January 2010).
[23] D.G. Johnson, *ibid.*
[24] Cesar Hidalgo, *Why Information Grows: The Evolution of Order from Atoms to Economies*, Basic Books, New York (2015)
[25] W.E. Bijker, *Ibid.*

rather than distributed and decentralised organisations[26]. The Internet is simply the 'network of networks' or 'a federation of networks able to communicate using TCP/IP network protocols through interconnected nodes'[27].Its short-term future projectsin several predictable directions, towards 5G, satellite broadcasting and Voice over Internet Protocol (VoIP), not to mention the IoT. In this scenario, those that control the infrastructure willalso control the data flow.

These factors converge to create a set of predetermined decisions made by default and by private entities with interests in how the community can access, participate, interact and decide over the technology –the Internet, in this case – and how these decisions affect the free, autonomous, informed participation of a democratic Internet[28].Thus, it is essential to address the connection between profiling and information control, with a focus on the socio-economic impact of the lack of legal harmonisation among the rules that govern these phenomena.

2. Profiling activities and the Net

2.1 What is profiling?

Profiling attaches a precise description to specific individuals, which allows for customisation of advertising, services, products, contents, and so forth and, above all, allows players to predict and influence behaviours[29]. For example, discriminatory pricing is a powerful tool adopted for this aim, showing different prices to different individuals for the same product/service at the same time, but based on the specific individual's profile. In the absence of Net Neutrality, this capability grants the power to decide precisely whether or not someone can access certain places of the Internet and the related content. Profiling was once the domain of criminal investigation by police (or authoritarian governments) only, whereas commercial players used targeting for their advertisements. Today, profiling and (micro)-targeting overlap in the infosphere[30], and their scope aligns to serve profit, power and control. Profiling is now an activity focused on inferring granular descriptive information about an individual (inferential data analytics). It aims to create as accurate a picture as possible of an individual's preferences, opinions, behaviours and other

[26] Theodor D. Sterling, *Democracy in an information society*, 4:1(2) The Information Society, (1986).
[27] Ennio Martinago, Vittorio Pasteris, Salvatore Romagnolo, ***Sesto potere***, Apogeo (1997).
[28] Cass R. Sunstein, *Deciding by Default*, 162:1 University of Pennsylvania L. Rev. 1-57 (2013).
[29] Custers, B.H.M. (2018) Data Mining and Profiling in Big Data, in B.A. Arrigo (ed.) The SAGE Encyclopedia of Surveillance, Security, and Privacy, p. 277-279, Thousand Oaks: SAGE Publications, Inc.
[30] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press UK, (2014).

personal characteristics[31]. It can be defined as the recording and cross-analysis of an individual's psychological and behavioural traits and patterns in order to assess and predict one's capabilities in a given sphere. Therefore, privacy is affected byeach stage of profiling, i.e. data mining, data collection and storage, data analysis and information extraction, profile usage and profile evolution (dynamic updating)[32].

2.2 The emergence of an emotional economy of profiling

In order to have value for data-miners, personal data must be measurable, i.e. being in the form of machine-readable structured data. Therefore, profiling is composed ofa measurable set of data categorisations and is limited to the collection of spontaneous activities- expressed or translated in data and metadata - that profiled individuals perform. Sensors on mobile devices have expanded the scope of this measurability, but profiling is still limited to what sensors can gather from daily usage. However, theIoT will see another level of expansion, as sensors will surround and monitor people 24/7 in the so-called smart ecosystem allowing full, constant and in-depth real-time profiling. Beyond this, the ultimate barrier might only be the human body and mind[33] which has already been described as 'pervasive profiling as social cruelty'[34].

User privacy is affected in all phases of data processing. Indeed, in recent years, profiling has moved from preference detection to prediction towards the next step of profiling transformation, which focuses on sensorial and emotional experiences. Profiling activities are expanding in scope, and the IoT will boost this transformation, allowing for whole users' 'passive-data' to be gathered. Passive-data is not only those data generated through active interaction with a device but those that represent all users' natural behaviours and characteristics captured by sensors (facial expressions, voice parameters and so on).We are in the "attention economy"[35], in which online platforms compete to attract users through personalised content and keep them in-the-loop using neuromarketing design features, such as scrolling (random rewards) and so forth. The result is that the more our attention is kept, the more we use the interface and

[31] WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 17/EN WP251rev.01

[32] Bert-Jaap Koops, *Some reflections on profiling: power shifts and protection paradigms*, in Hildebrandt & Gutwirth (eds.), Profiling the European Citizens, Springer, 326-337 (2008).

[33] Hassan Takabi, et. al., *Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures*, 2016 IEEE 2nd International Conference on Collaboration and Internet Computing.

[34] Sylvie Delacroix, Michael Veale, *Smart Technologies and our sense of Self: going beyond epistemic counter-profiling*, in O'Hara & Hildebrandt (eds.), Law and Life in the Era of Data-Driven Agency, Edward Elgar Publishing Ltd. (2019).

[35] See Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*, A. Knopf ed., Toronto, (2016).

generate data that can be profiled. Nonetheless, this paradigm is rapidly shifting to an 'emotional economy', in which content attractsusers in terms of the experience that it can generate. Simultaneously, platforms trackback an emotional profile that serves a twofold scope: on the one hand, a user's psychological profile is better tracked, and, on the other hand, the machine learning AI is trained to better 'understand' human emotions. For instance, Instagram stories are mined to nourish the so-called "Emotional AIs", using the biometric features of those who appear in the stories[36]. Meanwhile, Facebook has enhanced the "like" option allowing users to describe their state of mind connected with certain content. The ultimate aim is to better predict user behaviours for the forthcoming wave of interactive paradigm, i.e. Speech Interfaces (a.k.a. as Smart Speaker, Conversational Agents, Virtual Assistant and so on). In this scenario, it is relevant to explore the following equation: profiling intensity is proportional to the potential power that its knowledge generates, where power can be political, economic, strategic or, at least generally speaking, influential.

2.3 Legal analysis: the data-monetisation and profiling relationship loop

Research suggests that if we are not paying for it, then we are the product[37]; or more precisely, our data is the product. However, profiles have no value unless they can be analysed as structured data andthen attached to an identity (personal identifiable information - PII)[38]. Therefore, the more featuresthat can be attached to aPII, the more value the profile has: because identity is a commodity[39]. However, it must be acknowledged that IT professional stend to profile devices instead. This occurrence does not contradict the PII-profile relationship. Indeed, from an economic and computational viewpoint, there is no need to know who the end-useractually is. The important thing here is to be able to discriminate among different users (devices) where, essentially, users are considered solely as distinct units. Nonetheless, this ability to distinguish single units is precisely the identification power behind the concept of PII. Furthermore, for Data Protection law, it does not matter if the data controller identifies the devices or the individuals

[36] The "#10years challenge", i.e. the viral mood in which users published on Instagram and Facebook the comparison of their current picture with their picture of ten years before, is an example of how it can be trained an "ageing AIs" with public data.
[37] https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/(last visited June, 19 2019).
[38] https://www.technology.pitt.edu/help-desk/how-to-documents/guide-identifying-personally-identifiable-information-pii (last visited June, 19 2019).
[39] https://www.economist.com/science-and-technology/2019/05/23/online-identification-is-getting-more-and-more-intrusive(last visited June, 19 2019).

behind it, because the notion of "personal data" is purposely broad enough to coverall the activities in the spectrum:

"*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*[40].

As seen, profiling allows for content personalisation[41] enabling the customisations of users' digital experience. In turn, personalisation allows for discrimination[42]. Then, discrimination, in its negative connotation, can allow for an individual's isolation, although in some circumstances can create the potential for an individual's benefit over others. Isolation eventually creates thepotential for an individual's impairment: a weaker position means less bargaining power as well as less power to enforce one's rights. On the other hand, personalisation has value of personalisation when it comes to facilitating some users needs or desires, when freely chosen, consented to and autonomously expressed. Moreover, personalisation itself can be a positive discrimination tool, being required information in order to ensure or respect neutrality and equity to those individuals or situations that necessitate it.

From a Civil Law perspective, profiling activities establish a principal legal relationship among the data controller and the data subject. In general terms, this relationship is informed by two overlapping and sometimes conflicting domains, such as Private law[43] and Data Protection law. In turn, the Data Protection relationship under Private law can involve Contract law or Tort law depending on the type of relationship established (consent-based or legitimate interest-based). Contract law would also imply the application of Consumer law where the data subject is an individual who falls into that particular legal status according to the norm. On the other hand, profiling may entail Intellectual Property Rights (IPR) and Trade Secretsprotection on the data controller's side, as it may be claimed for inferential activities that entailthe data controller's intellectual work, opinions or techniques[44]. This might be valid, for instance, for a user's psychological profile created by the data controller. This profiledoes not need to be either exact or true, and the user (data subject) has no direct Data Protection rights on it, such as accessibility,

[40] GDPR article 4(1).
[41] Whatever it can be: service, information, product, access and so on.
[42] In terms of individuation and separation of an individual from the mass, in order to provide to him a particular treatment, different from the rest.
[43] Broadly speaking, as the civil matter that deals with every legal relationship between private parties.
[44] Gianluigi M. Riva, *Metadata, Semantic-data and their protection: legal nature and issues under the GDPR and the E-Privacy draft Regulation*, In 2018 Amsterdam Privacy Conference Proceedings.

portability, opposition and so on. At least, the GDPR does not provide any legal regime for it, specifically.

Leaving aside the legal specificity of these interrelations, it is crucial to highlight two aspectsof this study. First, there is an assumption that a 'data relationship' is established for a free service, in which service providers offer users access to certain services and, in exchange, users accept that their personal data will be processed. Second, and more importantly, this alleged gratuitous reconstruction is legally incorrect[45], as this relational paradigm expresses the elements of compensation between the parties, i.e. a synallagmatic contract. Furthermore, this involves many other layers of legal speculation, precisely on the nature and entity of this form of compensation. Indeed, users (or more appropriately, data subjects) yield their personal data, accept profiling, supply data controllers with new data - i.e. their attention[46], emotions and interactions – accept targeted advertising, endure indirect commercial exploitation (data-broking, price discrimination, credit issue) and possibly pay for accessing premium-features. In return users have access to the platform content, which is not neutral, as it isnot provided primarily as a user service but as a commercial tool to keep users online[47].The quantitative and qualitative value of these counter-compensations may exceed what is fair for the Law in these cases (good faith) because it creates unbalanced positions legally unacceptable for weak parties and consumers in Contract law. Furthermore, users are not explicitly informed about this kind of revenue model. Moreover, it must be considered that many of the platforms that engage in these kinds of data processing already require users to pay for products, e.g. Microsoft, Amazon, E-bay, Netflix, Airbnb, and Uber.

Another an essential element to consider in this data relationship, which is mandatory under Data Protection law, is that it is primarily based on the data subject's consent which, as noted, must be free, informed, and specific. Usually, the legal relationship established between the data subject and the data controller (i.e. the service provider) is affected by the monopolistic position of the latter and, most importantly, by the essential nature of the interactive service provided. Indeed, many social platforms (Facebook, Instagram, LinkedIn, Twitter and so on), communication tools (Browsers, Emails, WhatsApp, Messenger and so on), and services (Google Map, App Store, VoIP, Video Calls) can now be evaluated as essential goods, or at leastnecessary goods, covered by a social collective interest. Although it is possible to live without these goods, an individual could not actively and effectively participate in the society's mechanisms without them and would be missing out. If information is the water and the Internet is the aquifer, then

[45] At least according to the continental Civil Law tradition.
[46] T. Wu, *Ibid.*
[47]In this sense, see the Netflix paradigmatic tweet: "sleep is my greatest enemy"https://twitter.com/netflix/status/854100194098520064, (last visited September, 28 2019).

social media and browsers are the water wells in the desert: whoever controls them, controls life in the desert.

People are, to some extent, constrained to use these services by the net of social relationships and norms, despite the threat of the profiling 'trap'. Thus, the consent given for establishing these legal data relationships is not entirely free and autonomous but is instead determined by needs and decisions by default[48]. Therefore, through this lens, the data relationship is a 'non-contract', as the agreement, which is the primary element of a contract, is coerced by a functional requirement (data processing) to access an essential necessity. In this sense, it represents the mere ratification of a necessary requirement to access a service, and the individual only takes notice of the data processing with limited room for opting-in or -out to specific elements of the relationship. Note that the term 'necessary' here does not mean 'essential' but only refers to the necessary conditions as required by the service provider to provide its products or services.Some may argue that the user can choose not to engage in social platforms, or not to read long terms and conditions pages.This, however, would not be a real choice but a conditioned one, created by the combination ofweaker position and practical needs. Therefore, this is notgenuinely free consent asusersare not free to choose between a) accessing the essential goods without providing more personal data than necessary and b) accessing the service only by providing all data that can be gathered. It is actually a "take it or leave it" relationship[49], which is not only a trap but also a potential form of blackmail.

2.4 Profiling, manipulative influence and discriminatory pricing

Profiling activities already provide personalised content in which each user accesses different features without knowing why they appear to them or what others see. This is related to the psychological technique of "echo chambers"[50], in which platforms only show users content aligned with their profile[51]. It is also closely tied to discriminatory pricing[52]. It represents the capability to sell the same product to different people at a different price, which in turn is established on the basis of their profiles. This essentially means that price differences can vary based on a service provider's knowledge of users' desires or needs for products, as well as their

[48] C. R. Sunstein, *Ibid.*
[49] EDPS Opinion No. 3/2018 on online manipulation and personal data.
[50] Seth Flaxman et al., *Filter Bubbles, Echo Chambers, and Online News consumption*, 80 Public Opinion Quarterly (2016) Supplement, 298-320, 23 p. 4 Charts, 5 Graphs.
[51] Justin Farrell, *Politics: Echo chambers and false certainty*, 5:8 Nature Climate Change; London, 719-720 (Aug 2015).
[52] Paul Belleflamme & WouterVergote, *Monopoly price discrimination and privacy: The hidden cost of Hiding*, 149 Economics Letters, 141-144 (2016).

financial ability and willingness to pay for them. In a non-neutral Net system, this implies that lower prices products (or competitors' ones) could be shown overs lower broadband speeds, in favour of more expensive products on faster connections.The quality and ubiquity of platforms must also beconsideredas this power may be relevant regarding the potential threat of using these paradigms for silently blackmailing or punishing opponents, preventing them from accessing non-connected content, services or web places (for instance, in an authoritative system). This could be another (unethical) application of the "Nudge Theory"[53], which has already been implemented in profiling, by exploiting neuromarketing design techniques[54].Therefore, in a non-neutral Net, these unequal treatments can be boosted and combined, providing players with the enormous power of deciding the access flow and quality to content, or influence over users' choices.

2.5 Invasive and acceptable profiling

This dystopian situation could be already in place if there were an intention in this direction, but public opinion is unlikely to accept it, at present. Nevertheless, in a wholly dependent society driven by the IoT infrastructure, general attitudes to acceptability might change. Privacy paradox studies[55],[56] induce us to speculate that if we had been asked in the last century if we would have accepted that unknown people, employed by private industries, monitored all our correspondence, we would have probably responded negatively. In parallel, if we had been asked in the early 2000s, right after the advent of the smartphone, if we would share all our picture, personal contents and files with those same industries, we may have replied in a similarly negative manner. Now if we ask whether people are willing to be recorded and monitored in their daily activities, they would probably answer in the negative. For sure people want access to services and in order to have it are willing to bargain their intangible assets (personal data, which are not perceived as a commodity), especially, if the service is allegedly "free". However, over time people have continued to use email services, smartphones and invasive apps despite their privacy leaks, while these services switch to speech interfaces and wearables, which facilitate and implement further profiling. Contingent human needs drive acceptability in general and profiling

[53] Cass R. Sunstein, *Nudging: A Very Short Guide*, 37:4 J. of Consumer Policy, 583.588 (2014).
[54] Selena Semorin, *Neuromarketing and the "poor in world" consumer: how the animalization of thinking underpins contemporary market research discourses*, 20:1 J. of Consumption Markets and Culture, 59-80 (2017).
[55]Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41:1 The J. of Consumer Affairs, Madison, 100-126 (2007).
[56] Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, NBER Working Paper No. 23488, (June 2017)

acceptability in this particular scenario. We can rightfully argue that wearables fitness devices, for instance, are not contingent human needs, and people chose to be profiled in order to have a personalised service. That is true, but we must consider that individuals tend to accept the legal status quo of the terms and conditions, as they have no power to bargain them and, on the other hand, have no practical and immediate legal tools to fight abuses (precisely the Privacy paradox). Thus, they undergo the situation because "things work this way" and the market does it accordingly. Therefore, there is no real alternative if one wants (or needs) the service. This acceptability spectrum represents a kind of "Overton's window"[57], where humankind can get used to anything if dispensed slowly and in low dosages[58]. The role of the Law is not to forbid profiling but to protect users against abuses over their own coerced consent when it is yield in situations in which they are weak and in need.

Habits can shape bothhuman perception and acceptability of a given situation – even a bad one – and can be used accordingly to manipulate public opinion on a given phenomenon. This finds a connection with theinformation overload phenomenon, also known as "infobesity"[59], described as the constant and massive exposure to all kinds of information. The brain is continuously bombarded by new elements to be processed, without proper time to do it effectively orto reflect on this information[60].On the other hand, if bad behaviour spreads in society, people lose trust and start to accept it with resignation, because "that's how the world works". This resignation is in turn tied to ineffective regulations and loss of trust in institutions[61,62]. Numerous privacy scandals and the still non-compliant data processing of many digital applications reflect this phenomenon[63],and it is emphasised with those goods perceived as essentials-the "take it or leave it" blackmailing paradigm. Finally, regulatory systems that are unable to enforce their rules exacerbate these phenomena. Privacy perceptions are continuously undermined by uncompliant services, abuses, scarce transparency and regulatory gaps. With the

[57] https://en.wikipedia.org/wiki/Overton_window (last visited June, 19 2019), which is defined as the "range of ideas tolerated in public discourse, also known as the window of discourse". The concept states that an idea's political viability depends mainly on whether it falls within this range, rather than on politicians' individual preferences. Indeed, according to Overton, the window contains the range of policies that a politician can recommend without appearing too extreme to gain or keep public office in the current climate of public opinion. The range is formed by "unthinkable", "radical", "acceptable", "sensible", "popular", "policy", and describes the different stages of public perception.

[58] Chomsky's boiled frog concept. See note n. 53.

[59] Sebastian Groes, *Information overload in literature*, 31:7 Textual Practice, 1481-1508 (2017).

[60] S. Groes, *Ibid.*

[61] Gary Davies & Isabel Olmedo-Cifuentes, *Corporate misconduct and the loss of trust*, 50:7/8 Eu J.l of Marketing, 1426-1447 (2016).

[62] Siri Thoresen et al., *Loss of Trust May Never Heal. Institutional Trust in Disaster Victims in a Long-Term Perspective: Associations with Social Support and Mental Health,* Frontiers in Psychology (2018).

[63] Irish Data Protection Authority: DPC Annual Report 25 May - 31 December 2018.

IoT, our society may want to ultimately bargain its privacy rights for the sake of habits, comfort and resignation[64].

2.6 The 'profile and rule' concept in light of data scoring

Data profiling, monetisation and content personalisation are highly relevant for the Net Neutrality. First, the Internet can be represented as a chain of commercial interests, in which revenue models, profiling and derived profit are the three outermost rings. Therefore, in a web-based on 'Net discrimination', access to specific places on the web can be granted not only in respect to the content addressed but also to the data one accepts to yield for profiling.This scenario is already producing a data score history (comparable to credit history systems in the US[65] and China[66]) in which users are granted access to certain Net places or certain Net quality (speed and services) based on willingness to yield data and be profiled.

In consolidated credit systems, citizens are evaluated for their ability to acquire debt consistently and to fully repay these debts within the terms[67]. This system works by providing a score for debitcapability, where the rate is relevant to determine the level of accessibility to private (essential) services, such as medical insurance, rental accommodation, and mortgages. It spurs debtors to get into debt as early as possible to get a higher score and increase the debt amount in order to prove they can access a higher level of services[68]. In China, this is taken further with the social scoring system, in which some civic services are granted only to those that receive rates from their peers[69],[70]. If this is the potential scenario in which a profiling-driven Internet or discriminative-web points is possible and plausible, then we must also consider its incremental evolution within an IoT ecosystem. Indeed, the more people are isolated and monitored, deprived of bargaining power, assigned with a score that puts them in competition among each other, the more they can be controlled and influenced. This paradigm of

[64] Such as the Chomsky's boiled frog concept explains. https://en.wikipedia.org/wiki/Boiling_frog (last visited June, 19 2019).
[65] Calder Lendol, *Financing the American dream: a cultural history of consumer credit*, Princeton Un. Press, (1999).
[66] Wei Zhang et al, *China's Non-governmental Microcredit Practice: History and Challenges*, 31:3 J. of Family and Economic Issues, New York, 280-296 (Sep. 2010).
[67] https://observer.com/2018/02/america-isnt-far-off-from-chinas-social-credit-score/ (last visited June, 19 2019).
[68] https://eu.usatoday.com/story/money/columnist/powell/2018/07/05/credit-scores-9-things-know-how-its-calculated/736378002/ (last visited June, 19 2019).
[69] Yongxi Chen, Anne Sy Cheung, *The transparent Self under Big Data profiling: Privacy and Chinese legislation on the Social Credit System*, Journal of Comparative Law, 12:2, 356-378, (2019).
[70] http://time.com/collection/davos-2019/5502592/china-social-credit-score/ (last visited June, 19 2019).

user/service-provider relationship implies the 'profile and rule', which is the quintessence of the *divide et impera* restated for the IoT ecosystem.

3. Player power and the control of essential goods

3.1 Multi-monopolists

Today, substantial economic powers are concentrated in a few platforms. Their legal status is tied to the nature of their transnational ICT activities, so they supersede jurisdictions as extra-national entities. These so-called Giants hold key transversal market-positions in expanding territories. While the Law addresses the concept of monopoly concerning one field only, today, we have platforms that hold a set of monopolies or oligopolies in different fields[71], for example, Google (Alphabet). Therefore, the concept of a 'multi-monopoly' requires new Competition law rules. These multi-monopolies have elements in common: first, personal data and profiling is an asset for their core business; secondly, some[72] are expanding into finance with banking licences for e-payments; thirdly, some[73] are trying to become mobile Internet Service Providers (mISPs). How business entities consider their (personal) data assets reflectsthis phenomenon. For example, the 'data moat' isa protective strategic incentive forharvesting the most data possible[74] in order to gain a competitive advantage in creating the 'network effect'[75], a psychological-economicelement that helps create the multi-monopolistic cycle, informed and based on data mining and profiling.

3.2 How disinformation creates uncertainty and how both are tools of control

There are many breaches in the wall of userprotection. For example,a recognisable element of information (and disinformation) controlis represented by "fake news" where the connected commentary and demonisation of this phenomenon leverages public fears and a sense of

[71] Matthew Hindman, *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*, Princeton; Oxford: Princeton University Press, (2018).
[72] Google, Apple, Facebook, Amazon.
[73] Google, Amazon, Facebook.
[74] A 'Data Moat' is a competitive advantage that a business has thanks to its proprietary data set. It represents a modern example of traditional 'business moats', such as trade secrets, patents, know-how and so on. https://www.intricity.com/data-science/what-is-a-data-moat/ (last visited September, 27 2019).
[75] https://a16z.com/2019/05/09/data-network-effects-moats/(last visited September, 27 2019).

uncertainty.Many platforms takesignificant advantages from fake news, “fake reviews”and, more recently, “deep-fakes”[76] which allow them toboost viral mechanisms and gain from connected advertising revenues[77], creatinga behavioural eco-chamber mechanism used for a variety of business purposes[78], while the same platforms act as moderators in filtering information. This is another effect of echo-chambers which, along with denial, cognitive dissonance[79], and FOMO[80],[81] are utilised to keep users online in a profiling loop.

We live in both the information and disinformation age where the latter has a history as a deceptive communicative strategy for national security[82] or propaganda[83] and to an extent for marketing[84]. Nowadays, social media environments are raising the bar of information processability. In this scenario, someone could exploit some of the oldest tools of mass control: namely need, habitude and entertainment (*panem et circenses*[85]). If everything is information (knowledge), then nothing is information. Indeed, we can claim we live in the post-truth era[86].

Given this ‘fake-phobia’, people and government are askingprivate industries to play the role of truth-protectors and censors. They do not consider that we are asking those that control the information flow, to control also the information itself. This is a power previously only held by religious institutions in human history. Nonetheless, the article 17of the EU Directive on Copyright Law[87] indirectly asks players - and provides them with the power - to preventively engage in content-checking to ensure that IPRs are not violated. Therefore, it provides them with an ex-ante juridical power thatdoes not consider the range of freedom of speech and expression, which, in turn, comprehends fundamental rights such as freedom of press, political satire, free

[76] A facial re-enactment technique that falsifies videos and voices making people appearing as they act in the video, while they are not. https://www.youtube.com/watch?v=ohmajJTcpNk&t=28s(last visited September, 27 2019).

[77] Joshua A. Braun & Jessica L. Eklund, *Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism*, 7:1 Digital Journalism (2019).

[78]https://www.businessinsider.com/open-banking-will-facebook-google-and-amazon-get-into-finance-2018-1?IR=T (last visited June, 19 2019).

[79] Eddie Harmon-Jones (Ed*), Cognitive dissonance: Reexamining a pivotal theory in psychology* (2nd ed.) § xvi, 303, Washington, DC, US: American Psychological Association, (2019).

[80] “Fear of missing out”.

[81] Sarah Buglass et al., *Motivators of online vulnerability: The impact of social network site use and FOMO*, 66 Computers in Human Behavior, 248-255 (2017).

[82] Roberto Garcia Ferreira, *The CIA and Jacobo Arbenz: History of a disinformation campaign*, 25:2 J. of Third World Studies (2008).

[83]https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf(last visited June, 19 2019).

[84]http://theconversation.com/the-manipulation-of-the-american-mind-edward-bernays-and-the-birth-of-public-relations-44393 (last visited June, 19 2019).

[85] Literally: “bread and circus”, meaning to give people what they need to fill the stomach and what to entertain the mind avoiding they think about other things.

[86] Sergio Sigismondo*, Post-truth?*, Social Studies of Science,47:1, 3-6 (2017).

[87] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

speech, usage of public images and so forth.It cannot be known[88],[89] if this is the result of lobbying pressures on the EU Parliament.There is however another parallel with the GDPR, that amplified the role of individual's consent and deprived it by the (direct) protection of other essential elements, such as the principle of necessity, of purpose, and minimisation[90]. Indeed, GDPR article 6(1) a) expressly states that data subject's consent is sufficient alone to render the data processing lawful[91]. It implicitly means that if the data processing lacks the application of the listed principles, it is, however, lawful if there is the consent. Nevertheless, despite its central role in the GDPR, consent remains highly subject to influence, coercion and manipulation. Indeed, it is one of the weakest forms of protection for individuals, and that is the reason why Consumer law protects individuals from vexatious clauses even if they accepted them.

3.3 Zero-rating and social credit scoring

Zero-rating connections, which can be considered another form of "take it or leave it" practice[92], might be the tools to maintain an illusion of freedom concerning neutral Net accessibility. Zero-rating was silently and non-expressly introduced in the EU regulation 2015/2120, possibly to temper the principle of Net Neutrality and allow players to ask users to pay for higher quality services. However, the norm is biased by the assumption that these services are free, where actually service providers are richly compensated in personal data, as seen. Multi-monopoly players could easily introduce a data score system that mimics social identity behaviours (likes, revisions, online activity rate) and profiling inclination, in order to evaluate user ability to yield data, i.e. the ability to generate PII for inferring analysis. Aside from the Net Neutrality domain, this data scoring is already a practice for the digital services described so far. In such scenarios, it is unclear if attributing a score to individuals must be considered by Data Protection as inferring data activity or a judgment. In the first case, it may be possible for data subjects to apply their right of opposition and so on, although with several limits and clashes with IPRs[93]. In the second case, Data Protection rights would not apply, because judgment is a legitimate opinion – meaning

[88] https://www.asktheeu.org/en/request/facebook_lobbying_gdpr_2 (last visited June, 19 2019).
[89] https://iapp.org/news/a/inside-the-eprivacy-regulations-furious-lobbying-war/ (last visited June, 19 2019).
[90] G. M. Riva, *ibid.*
[91] In this sense, cf. the combined literal provisions of GDPR article 6(1) a) and article 5(1) a): consent is alone sufficient to render the data processing lawful, while transparency, necessity and all the other principles do not concur in forming the lawfulness of the data processing.
[92] WP29 Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). 17/EN WP 247
[93] G. M. Riva, *ibid.*

freedom of expression - made by a private entity and as such, cannot be banned[94]. In this data scoring scenario, zero-rating services might be introduced precisely to let people pay with profiling rather than money, which might be fair[95].Only, it may genuinely be considered fair within the context of a higher standard of Data Protection, not merely based on the consent rule, and in which the centralisation of powers is tempered and governed by democratic institutions, rather than private entities. Without proper borders, zero-rating may represent another bypass of the consent-rule, allowing players to introduce a lawful "take it or leave it" position that can be conjugated into elimination of ad-blocking, necessary acceptance of cookies, invasive profiling and so on[96]. Essentially, it would be the negation of Privacy by Default principles.

3.4 Mass customization through pricing personalization and discrimination

Pricing discrimination means that players can sell the same service or product with a personalised price to two different people, based on their profiles and history. This implies the antithetical power of 'mass customisation', i.e. the ability to personalise features for every single individual (micro-target) that composes the mass (persona, target or cluster), disguising it as a mass-targeting. In terms of Private law in Civil Law systems[97], several questions arise about both Contract and Consumer laws. According to the Civil Code[98], the contract - although telematic - follows the scheme of proposal and acceptance. This scheme falls into the legal regime of the "offer to the public"[99], which states that a public offer that has the essential elements for a contract[100] involves a contractual offer and can be revoked only in the same ways it was published. Neither the Directive on Consumers' rights[101] nor the Civil Code state that the price

[94] Sandra Wachter & Brent Mittelstadt, *A Right to reasonable inference: Re-thinking Data Protection Law in the age of Big Data and AI*, 2019, 1 Columbia Business L. Rev.
[95] BJ Ard, *Beyond Neutrality: How Zero Rating Can (Sometimes) Advance User Choice, Innovation, and Democratic Participation*, 75:984 Maryland L.Rev., 984-1028 (2016).
[96] Jessica A. Hollis, *Testing the bounds of the Net neutrality with Zero-rating Practices*, 32:591 Berkley Tech. L. Rev., 591-620 (2017).
[97] Here the reference is to the Italian Private Law, as an example of contractual legal regime in the EU Civil Law systems. https://wipolex.wipo.int/en/legislation/details/16608. (last visited June, 19 2019). Other Member State national legislations may have similar norms.
[98] Italian Civil Code, article 1326 "Conclusion of the contract"
[99] Italian Civil Code, article 1336 "Offer to the public"
[100] And price is one of them.
[101] Directive (EU) 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

must be the same for all the customers. This is tied to the fact that the norms assumed it as a factual element, given that they were drafted in a fully offline society.

However, for offline transactions, the national law[102] requires that dealers must show the prices of the offered goods. For offline realities, the circumstance was implicit: a shop could not physically make public a different offer for different customers preventing them from seeing other prices (publicy). In terms of E-commerce platforms, in which players sell services or products with pricing discrimination, there are several issues to consider. First, as it is an online space, offline rules canapply via legal analogy. Secondly, EU and national contractual norms for contracts by adhesion and, in general, off-premises contracts[103] apply, even if article 4(4) states that transactions below 50 Euros do not apply and in any case must be considered telematics contracts[104]. Thirdly, it is open to question if the offer must be considered public or private, as the price is formed only for that particular customer, even though the goodsare offered publicly. However, it can be argued that while the price is private, the overall offer of the product is public. However, this is an assumption that can only be proved by the dealer and, to be considered as a public offer, must have all the essential elements of a contract, with the price being one of them. Then, there is the question of whether the discriminatory price can be considered as a vexatious clause, which is null for EU Consumer law. Here, however, Consumer law itself may not apply, as noted above, and yet, if the price determination is null, the entire contract is null, as the price is an essential element for its existence and therefore its validity.

Help may arrive from two specific dispositions. The first is the "obligation to contract in case of monopoly"[105] which requires that those enterprises which are in the position of a (legal) monopoly, have to contract with whoever adheres to the offered services and with the same conditions. Nevertheless, this rule applies to essential services in amonopoly regime. Hence, it can be argued that it applies only to recognised monopolies[106] (and not to oligopolies) as well as only to those who offer essential services, and so standard products or services should be excluded. This reveals the regulatory gap concerning multi-monopolies, which are not considered by the law. The second aspect to consider is that information and social platforms can be considered as essential goods for self-determination, self-expression and, above all, social

[102] Italian Legislative Decree 114/1998. Others EU Members might have similar rules in their respective national laws.
[103] Directive (EU) 2011/83 article 5.
[104] Which, however, should be comprehended in off-premises contracts, as per recital 22 of the Directive.
[105] Italian Civil Code article 2597.
[106] EU Court of Justice: Akzo Chemie C – 62/86 (1991) established a presumption of dominance where the enterprise holds at least 50% of the market.

engagement. This concerns Competition law[107] and specifically the "abuse of dominant position"[108] towards consumers[109]. However, it involves a "distortion of the market" so we must discuss what can be considered as "distortion" in this context and if price personalisation falls into that definition. However, it must be highlighted that the abuse of dominance is of concern, but not the dominance per se.

There are also other national norms forbidding discriminatory prices that would suit this legal situation, as they regulate the abuse of economic dependence[110], but they apply only between enterprises. However, the cited disposition is based on the legal concept of the prohibition of the abuse of the right, which can also be considered a general principle of the EU legal system[111]. The issue is to determine what kind of conduct constitutes abuse, as it is actually based on profiling. If based on the data subject's consent or performed on another legal basis, it is lawful. Here the relevance of harmonisation among regulations emerges, as there is no coordination between Data Protection law, Competition law and Consumer law. Furthermore, there are grey areas that can be easily exploited for abuses, although legally justifiable. This lack of coordination with the zero-rating rules and their general character also creates further relevant gaps.

4. Neutral accessibility privacy by design solutions

4.1 The right to access content as a form of ingress-egress over a digital easement

A neutral Net is such when everyone can exploit the same connection independently of their characteristics, statuses or aims. Neutral access to the Internet may be instead defined as the right to access (use) the tool, while the ability to reach the content of choice can constitute a legitimate interest, meaning an expectation. Thus, Net accessibility representsthe right to access the tool, but not to possess it; meaning that the service supplier cannot keep an individual from accessing it. However, individual shave no right to have an Internet connection, reflecting the

[107] Articles 101 and 102 TFEU: Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01
[108] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (TFEU)
[109] Italian Law 287/1990 article 3(b) (Competition Law)
[110] Italian Law 198/1998 article 9.
[111] CFREU Article 54: Charter of Fundamental Rights of the European Union 2012/C 326/02

same tiny difference that exists between the right to participate inacompetition but not to win it. The first is a right; the second is an expectation. The right to accessibility should refer both to the service supplied (the broadband) but also to the content (being able to reach a precise domain) if it is publicly available. A parallel example can be electricity, in which one has not only the right to be supplied at the same conditions, with a certain quantity of electricity, but also to use it for whatever purpose, whether the TV or the laptop. Therefore, there is an intrinsic quantitative and qualitative aspect of the concept of accessibility[112]. Accessibility may even be extended to the semantic understanding of the purpose of the access itself, as accessibility does not imply a moral judgment. The content a user aims to reach does not need to be defined as good or bad, true or false, in order to have a legitimate legal interest in reaching it.

Hence, one may be entitled to enforce the same right of accessibility for either verified or fake news. This concept may be grounded on the legal assumption of the Net as an essential public good, on which hangs the collective interest of neutral usage, i.e. access for specific purposes. Indeed, today the Net has all the elements necessary to be considered an essential good for society and individuals, as it is not only a tool to access information but also a way of communication for the expression of one's self-determination. Online profiles explicate this freedom of expression. Furthermore, as the World Wide Web was never patented by the CERN, it can be argued that once rendered accessible, it became an available public good. Further, and for analogy, during the time it has been accessible, it has constituted a public ingress-egress over easement entitlements[113] as a virtual passageway.

The hermeneutical issue is that ingress-egress right is a "real right"[114] of usage and can be applied only to material goods. On the other hand, it can be argued that the Net is made of material cables and servers in which cyberspace is only one of the dimensions, such as the legal concept of "entries"[115] for terrains (representing the ethereal space in which sounds, smoke and liquids travel through a territory).Thus, under this legal scheme, there would be a public right to accessibility through the Net, in order to reach one of its dimensions. With this, neutrality might be referred to as accessibility not only in a quantitative and qualitative way but also in other dimensions. Horizontal accessibility would represent the ability to surf the web, as the overall dimension of the material Net (the broadband), while vertical accessibility would represent the

[112]Friederike Kerkmann, *Web Accessibility*, 36:455 Informatik Spektrum (2013).

[113] What is defined, literally, as predial servitude of passage, meaning the right to access others' propriety in order to pass and reach a certain point. The latin term "praedium" (terrain), is important as it means that the right exists in relation to the terrain, and not as a personal benefit.

[114] i.e. a Civil Law categorisation for those rights that are expressly provided by the Law, direct toward the good and absolute, meaning that can be enforced over anyone.

[115] Italian Civil Code, article 844. "Entries" are considered those immaterial conditions such as heat, smell, smoke, noise that might derive from a material good.

capacity to access different dimensions of the cyberspace, such as websites, or DSN or specific sensors. Therefore, if the Net was the press and the Web was a newspaper, the quantitative aspect of the right of accessibility would be an entitlement to buy, under the same conditions as others, a subscription to the newsstand catalogue. The qualitative aspect would be the ability to access one specific newspaper and its content, while the horizontal accessibility would be represented by the possibility to access every newspaper indexed in the catalogue. Finally, vertical accessibility would be represented by the ability to access article sources and references and other articles from the same author. Nevertheless, having a right to access any content should not preclude the counter-interest of both players and users of accessing the 'best' content in the 'best' way and for players to monetise the service.

4.2 Data accessibility and 'Neutrality by Design'

These theoretical accessibility features may become relevant when it comes to IoTand 5G neutrality. Indeed, the right of access is one of the Data Protection procedural rights accorded to data subjects under certain conditions[116]. This refers to personal data and is connected to data portability[117]. Indeed, knowing the quantity, quality and location of personal data is a substantial precondition forenforcing that right in practice. Accordingly, the hermeneutical harmonisation between Data Protection, Consumer and Competition law, as well as Private law, may provide interpretative tools to ensure a fully neutral Net accessibility even in IoT ecosystems. Moreover, it may represent a remedy to mass customisation of services and products, whereas profiling abuses may be balanced by effective, enforceable rights in a 360-degree legal spectrum.

The same conceptual form of access seems to be granted by the BEREC guidelines[118] when referring to the connectivity to virtually all endpoints of the Internet. Similarly, the regulation[119] precisely states that users have the right to access and distribute information and content, to use and provide applications and services, and to use terminal equipment of their choice, irrespective of end-user or provider location or the location, origin or destination of the information, content, application or service, via their Internet access service. Nonetheless, it must be noted that BEREC

[116] GDPR, article 15.
[117] GDPR, article 20.
[118] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, 2016, BoR (16) 127, as provided by Article 5(3) of the Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.
[119] Reg. 2015/2120 article 3(2).

guidelines understand the term “Internet” as referring to a global system of interconnected networks that enables end-users to connect each other, i.e. limiting the accessibility to the communicative connection among two users[120].

4.3 Regulatory harmonisation

Notably, the current BEREC guidelines state that the Regulation observes the fundamental rights and principles of the Charter, concerning the protection of personal data, the freedom of expression and information, non-discrimination and consumer protection[121] (ref. Recital 33). However, a relevant gap between regulation and the real-world remains, especially concerning newer technologies. Concrete harmonisation would require an international regulatory framework to establish unique and shared rules for the same global phenomenon. Furthermore, there is areal need for extending the limits of merely formal requirements, by implementing substantial and enforceable positions, thus developing the concept of ‘democracy by design’. However, context is everything, and the Law cannot be regardedanymore as a static domain. The power of legal concepts resides in their application to new phenomena using interpretative tools such as the legal analogy. Unfortunately, it is not sufficient to fill existing gaps with hermeneutical speculations of legal scholarship, while waiting for the Courts to receive them in legal reasoning and for lawmakers to implement them in regulations. This process would take years. There is however an urgent need for a shared European legal harmonisation of these issues, if not even a moreambitious project involving a European common private law codification, built upon the continental traditions of civil codification.

4.4 Privacy by Design with user-in-control solutions

A practical solution can address these issues by rendering the interactive design of platforms more accessible to users. In this way, the design of features, interaction with specific content, orthe frequency and quality of adsas well as the degree of personalisation, would be transparent for users. This Privacy by Design approach would empower users with full control over accessible content and related profiling activities. While platforms currently offer users whatever they want, there is no way for users to know why certain content is displayed instead of other content. Instead, users should be able to select the type of interaction they want to perform while being

[120] BEREC n. 14 p. 6.
[121] BEREC n. 20 p. 7 and Reg. EU 2015/2120 Recital 33.

empowered with more consistent information over their personalised content. PbD means that platforms implement adesign-feature to show – on request – why the user is being presented with particular content, features or advertisements. In general, it may be argued that if a content filter has to be in place, it should not be in the hands offor-profit entities. However, a possible solution to preserve content neutrality and accessibility would be to also flag the content[122], providing users with interactive tools to check the source, provider and relevant production information (publishing date, physical source and so on). This solution would empower users with the distinction between information, misinformation and disinformation, putting them in the position to decide whether to rely on it or not.

5. Conclusion

This study has investigated the different interrelated aspects that connect Net neutrality to Data Protection. Given the tremendous influential power of Internet entities and their economic position, lawful activities such as profiling, zero-rating, discriminatory pricing, and information filtering can be easily abused. This potential power of influence is only unlawful when used against weaker parties. While Internet companies must not be considered guilty of holding this power, the concentration of too many powers in too few entities must be addressed preventatively by the Law. This should avoid misleading practices and allow commercial players to organise their activity in accordance with regulatory provisions.

This investigation shows how the current regulatory framework already protects users for unique legal situations but needs a normative intervention to coordinate the existent body of norms. The harmonisation would strengthen the tools for enforcing users' rights, both individually and collectively. As shown, this "positive" legal intervention should connect the spectrum of consumer, data subject and contractual party protection. The analysis demonstrates that the chain of revenue models, multi-monopolies, Net Neutrality rules, profiling and data protection, represents a loop that only regulatory harmonisation and PbD policies can breach. In this sense, democratic participation needs to be enhanced with a neutrality-by-design programme to support the accessibility of the Net (of things).

Future works may point in the direction of connecting the different legal branches touched in this work, through the analysis of Courts decisions and case law studies. Besides, this work paved the ground for addressing more specifically the topic of information control in a

[122] During the reviewof this study, Twitter announced that is going to flag Deep-fake contents without deleting them. See https://techcrunch.com/2019/11/11/twitter-drafts-a-deepfake-policy-that-would-label-and-warn-but-not-remove-manipulated-media/(last visited November, 11 2019).

combined interdisciplinary analysis, which stands at the intersection among Law, Ethics and Human-Computer Interaction. Also, education plays a central role in information management, and the lack of sufficientlegal knowledge among stakeholdersshould be investigated in relation to the scenarios described.

Information is and always will be something powerful, while knowledge is and always will be something useful and wise. Unfortunately, we live in the age of information, not yet of knowledge.

References

ALCOTT, Hunt; GENZTKOW, Matthew. *Social Media and Fake News in the 2016 Election,* 31:2 J. of Economic Perspectives, 211–236 (2017).

ARD, BJ. *Beyond Neutrality: How Zero Rating Can (Sometimes) Advance User Choice, Innovation, and Democratic Participation*, 75:984 Maryland L.Rev., 984-1028 (2016).

ATHEY, Susan et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, NBER Working Paper No. 23488, (June 2017).

BELLEFLAMME, Paul; WOUTERVERGOTE, *Monopoly price discrimination and privacy: The hidden cost of Hiding*, 149 Economics Letters, 141-144 (2016).

BIJKER, Wiebe E. *How is technology made?—That is the question!*, 34:1 Cambridge J.of Economics, 63-76 (January 2010).

BRAUN, Joshua A.; EKLUND, Jessica L. *Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism*, 7:1 Digital Journalism (2019).

BUGLASS, Sarah et al., *Motivators of online vulnerability: The impact of social network site use and FOMO*, 66 Computers in Human Behavior, 248-255 (2017).

CHEN, Yongxi; CHEUNG, Anne Sy. *The transparent Self under Big Data profiling: Privacy and Chinese legislation on the Social Credit System*, Journal of Comparative Law, 12:2, 356-378, (2019).

CUSTERS, B.H.M. (2018) Data Mining and Profiling in Big Data, in B.A. Arrigo (ed.) The SAGE Encyclopedia of Surveillance, Security, and Privacy, p. 277-279, Thousand Oaks: SAGE Publications, Inc.

DAVIES, Gary; OLMEDO-CIFUENTES, Isabel. *Corporate misconduct and the loss of trust*, 50:7/8 Eu J.l of Marketing, 1426-1447 (2016).

DELACROIX, Sylvie. Michael Veale, *Smart Technologies and our sense of Self: going beyond epistemic counter-profiling*, in O'Hara & Hildebrandt (eds.), Law and Life in the Era of Data-Driven Agency, Edward Elgar Publishing Ltd. (2019).

FARRELL, Justin. *Politics: Echo chambers and false certainty*, 5:8 Nature Climate Change; London, 719-720 (Aug 2015).

FERREIRA, Roberto Garcia. *The CIA and Jacobo Arbenz: History of a disinformation campaign*, 25:2 J. of Third World Studies (2008).

FLAXMAN, Seth et al., *Filter Bubbles, Echo Chambers, and Online News consumption*, 80 Public Opinion Quarterly (2016) Supplement, 298-320.

FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press UK, (2014).

FUERTES, Mercedes. *Endefensa de la neutralidad de la red*, 99:100 R.V.A.P., 1397-1412 (2014).

GROES, Sebastian. *Information overload in literature*, 31:7 Textual Practice, 1481-1508 (2017).

HARMON-JONES, Eddie (Ed). *Cognitive dissonance: Reexamining a pivotal theory in psychology* (2nd ed.) § xvi, 303, Washington, DC, US: American Psychological Association, (2019).

HIDALGO, Cesar. *Why Information Grows: The Evolution of Order from Atoms to Economies*, Basic Books, New York (2015)

HINDAM, Matthew. *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*, Princeton; Oxford: Princeton University Press, (2018).

HOLLIS, Jessica A. *Testing the bounds of the Net neutrality with Zero-rating Practices*, 32:591 Berkley Tech. L. Rev., 591-620 (2017).

JOHNSON, Deborah G. *Democracy, Technology, and Information Societies*, in: Philippe Goujon et al. (eds.), *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleurs.j.*, 233 IFIP International Federation for Information Processing, Springer, Boston, MA, (2017).

KOOPS, Bert-Jaap. *Some reflections on profiling: power shifts and protection paradigms*, in Hildebrandt & Gutwirth (eds.), Profiling the European Citizens, Springer, 326-337 (2008).

KULATHURAMAIYER. N.; BLAKE, W.T. *Restricting the View and Connecting the Dots - Dangers of a Web Search Engine Monopoly*, 12:12 J. of Universal Comp. Sc., 1731-1740 (2006).

LENDOL, Calder. *Financing the American dream: a cultural history of consumer credit*, Princeton Un. Press, (1999).

MARINAGO, Ennio. Vittorio Pasteris, Salvatore Romagnolo, ***Sesto potere***, Apogeo (1997).

NORBERG, Patricia A. et al., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41:1 The J. of Consumer Affairs, Madison, 100-126 (2007).

ODIFREDDI, Pier Giorgio. *La democrazia impossibile*, in: Ciro Ciliberto & Roberto Lucchetti (eds.), *Un mondo di idee*, I blu (pagine di scienza), Springer, Milano, (2011).

RAMPINI, Federico. *Rete padrona. Amazon, Apple, Google & co. Il volto oscuro della rivoluzione digitale*, Feltrinelli, (2015).

RHEINGOLD, Howard. *The Virtual Community. Homesteading on the Electronic Frontier*, Reading: Addison-Wesley, (1993).

RIVA, Gianluigi M. *Metadata, Semantic-data and their protection: legal nature and issues under the GDPR and the E-Privacy draft Regulation*, In 2018 Amsterdam Privacy Conference Proceedings.

SEMORIN, Selena. *Neuromarketing and the "poor in world" consumer: how the animalization of thinking underpins contemporary market research discourses*, 20:1 J. of Consumption Markets and Culture, 59-80 (2017).

SIGISMONDO, Sergio. *Post-truth?*, Social Studies of Science,47:1, 3-6 (2017).

STERLING, Theodor D. *Democracy in an information society*, 4:1(2) The Information Society, (1986).

SUNSTEIN, Cass R. *Deciding by Default*, 162:1 University of Pennsylvania L. Rev. 1-57 (2013).

_____. *Nudging: A Very Short Guide*, 37:4 J. of Consumer Policy, 583.588 (2014).

TAKABI, Hassan et. al., *Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures*, 2016 IEEE 2nd International Conference on Collaboration and Internet Computing.

THORESEN, Siri et al., *Loss of Trust May Never Heal. Institutional Trust in Disaster Victims in a Long-Term Perspective: Associations with Social Support and Mental Health,* Frontiers in Psychology (2018).

WACHTER, Sandra; MITTELSTADT, Brent. *A Right to reasonable inference: Re-thinking Data Protection Law in the age of Big Data and AI*, 2019, 1 Columbia Business L. Rev.

WU, Tim. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*, A.Knopf ed., Toronto, (2016).

ZHANG, Wei et al, *China's Non-governmental Microcredit Practice: History and Challenges*, 31:3 J. of Family and Economic Issues, New York, 280-296 (Sep. 2010).

Acknowledgements

This research was funded under the EU Horizon 2020 scheme of Marie Sklodowska-Curie Action grant agreement No. 722561.

G.M. Riva thanks Dr Luigi Panzeri for his helpful perspective on the IT side of the matters addressed. He also thanks Darragh McCashin for his precious opinions on the psychological implications of the study. Both have no responsibility for the content.

.....

Gianluigi M. Riva
Gianluigi M. Riva is a Marie Curie Ph.D. fellow in Privacy, Ethics and New Technologies at the University College Dublin, School of Information and Communication with a project on invasive technologies and consent-manipulation. Currently, he is performing his secondment at Telefonica Innovaciò Alpha in Barcelona, Spain, to develop Ethics and Privacy by Design guidelines in Human-Computer Interaction. He is an attorney at Law at the Italian Bar and acertified DPO.

Marguerite Barry
Marguerite Barry is Assistant Professor at the School of Information and Communication Studies of University College Dublin, where she teaches courses such as Information Ethics, Digital Storytelling and Organisation & Retrieval of Information. Her research interests focus on ethics in human computer interaction (HCI), technology and well-being, discourses on science, technology and society (STS) and histories of digital media.

.....

Enviado em: 07 de agosto de 2019

Aprovado em: 16 de novembro de 2019