Do we Need a Political Economy of Surveillance? The Case of the GDPR: A Critical Account of the Norms Governing Cyberspace

Francesco Lanzone[1]

ABSTRACT

This study examines the General Data Protection Regulation of the European Union from a critical perspective. By doing so, it aims to generate a comprehensive account of online surveillance practices for commercial purposes, and how public policy in this field is normatively conceived. In order to untangle the normative elements of this highly contested and complex regulation, which took more than five years to be signed under intense lobbying, this paper concentrates on the topics of Consent, Data Ownership and Profiling. These three interrelated elements constitute the primary sources of power asymmetries in the Web between users and providers of online services. By employing the proposed theoretical perspective of a political economy of surveillance, this paper draws from concepts of Foucauldian panoptic surveillance and of Marxist political economics, in order to draw a picture of current surveillance practices by major, quasi-monopolistic IT corporations such as Google and Facebook. The analysis then tests this framework with regard to the normative stance taken by the GDPR, the first major initiative aimed at regulating cyberspace. Deconstructing regulation in this way helps to understand the normative and ideological lines of action of the EU in the newly emerged policy area of the Common Digital Market.

1. Introduction

> *"The spectacle, grasped in its totality, is both the result and the project of the existing mode of production. [...] In all its specific forms, as information or propaganda, as advertisement or direct entertainment consumption, the spectacle is the present model of socially dominant life. It is the omnipresent affirmation of the choice already made in production and its corollary consumption."* (Guy Debord, 1967)

In recent years, terms such as The Age of Big Data, Network Society or Surveillance Society have come to be associated with an ever-growing relevance of information technologies in contemporary societies. Major scandals such as the Cambridge Analytica leaks and the Snowden revelations have contributed to the perception that a dangerous overreach and unaccountability of surveillance practices has become a global problem that needs to be tackled (Regan, 2012). In particular, the practices of major IT corporations such as Google and Facebook have sparked numerous controversies, due to a business model which some scholars argue represents a broader trend in the development of the digital environment towards a capital accumulation model based on surveillance (Cohen, 2008).

In Europe, national and supranational institutions have dedicated resources and invested political capital in devising a policy response to the risks posed to the wider fabric of society by these technological innovations. The more prominent example being the recent entrance into force of the EU General Data Protection Regulation (hereinafter referred to as "EU GDPR", or "the Regulation"), a highly controversial legislative instrument, which took more than four years to be approved and was subject to over four thousand proposed amendments under intense lobbying (Baker, 2013; Spiegel Online, 2012). This

[1] Francesco Lanzone received a bachelor degree in European Studies at Maastricht University in 2018. At the moment, he takes a Double Degree in Public Policy at Sciences Po Paris and Hertie School of Governance Berlin. Contact: francesco.lanzone@mail.com

controversy can be explained by the fast diffusion of these technological developments and the relevance of this sector for EU economies. Indeed, we are living at a time of history when around 3 billion people have access to the internet, producing an amount of data which can fill 10 million blue ray discs in a single day (Walker, 2015). While data now represents a source of value, it also represents a source of power (Mantelero, 2013), with far-reaching implications on society and politics.

As data collection and processing techniques are acquiring more and more relevance in the lives of citizens, the space for the enactment of inequitable power relations has increased as a result of an expansion of these technologies, both between the state and the citizen as well as between the citizens and private organizations. It is therefore necessary to provide a critical account of these phenomena from an interdisciplinary perspective in order to grasp the underlying power structures that these dynamics engender. Previous research on the topic from the perspective of surveillance studies has criticised the current development of digital surveillance practices from a sociological and philosophical perspective, exploring its effects on society at large, especially regarding the human right to privacy (Cohen, 2015; Hull, 2015). From the perspective of critical studies and Marxist political economics, previous research has identified the business models of major IT corporations as an example of the replication of neoliberal modes of development into the domain of the internet, in a process which engenders new forms of exploitative power-relations (Fuchs et al., 2013). However, such approaches have either concentrated on the philosophical and historical aspects of the phenomenon, or on their political and economic implications.

The present study aims to combine insights from these disciplines to develop a holistic and interdisciplinary critique of contemporary surveillance practices by major IT corporations such as Google and Facebook, building on the previous work of Gandhi (1993) and Fuchs et al. (2013) towards this direction. The proposed theoretical perspective is that of a "political economy of surveillance", which consists of a set of interrelated concepts relating to the way in which major IT corporations collect and analyse data in a practice of surveillance, in order to generate profits through an economic model based on targeted advertisement and profiling. This thesis tests the theory of a political economy of surveillance by looking at the case provided by the policy instrument of the EU GDPR, as it represents a major initiative in the definition of the norms governing the cyberspace. It does so by exploring the following research question: To what extent does the political economy of surveillance apply to the EU General Data Protection Regulation?

The first section addresses the proposed theoretical framework of a political economy of surveillance, in an effort of theory building based on relevant contributions from the domains of critical theory, surveillance studies and Marxist political economics. The second section addresses the various concepts on which the theory is based, namely consent, data ownership and profiling, which are outlined and operationalised. It ends with an acknowledgement of the methodological choices and their relevant limitations, together with an account of the chosen case, by detailing the necessary background information and expressing the relevance of such case selection. Thirdly, the paper performs an analysis of the GDPR through the lenses of the identified framework, with the support of relevant secondary legal sources, in order to uncover whether the described phenomena are reflected in the normative stance of this legislative instrument. In conclusion, it provides an overview of the findings and their broader implications for the study of contemporary developments in information technologies from a critical perspective.

2. Conceptualizing a Political Economy of Surveillance

This chapter aims to elaborate a conceptualization of the current developments in information technologies, drawing from relevant contributions from the domains of critical theory, political economics and surveillance studies. It firstly addresses, through the lens of the Foucauldian Panopticon, why the mechanisms of surveillance apply to the contemporary advertisement ecosystem, and the intersection of those practices with the concept of the producer-consumer developed by Marxist political economists. Secondly, the issues of consent, data ownership and profiling are addressed by drawing from these disciplines in order to form a sufficiently precise conceptualization of the interrelated dynamics that compose the proposed framework of a political economy of surveillance. Such an approach is grounded in the need for a holistic and critical conceptual toolkit to address the current issues that the information society is facing, such as online surveillance and intrusive profiling.

The proposed conceptual framework of a political economy of surveillance encompasses the current practices of data collection and analytics of corporations such as Google and Facebook, which belong to a wider advertising ecosystem (Turow & Draper, 2012). The advertising ecosystem is composed of a variety of actors such as social media platforms, who profile users on the basis of their activity on the site, and data brokers[2], who gather and distribute advertisements over a number of affiliated sites by targeting them at consumers through profiling practices based on the use of cookies[3] and other identifiers (Elmer, 2003). The development and progressive assertion of these platforms as the dominant actors on the Web has engendered numerous debates at the academic, political and economic levels, often sparked by controversies and scandals. By bringing forward the concept of a political economy of surveillance, the present paper draws from an elaboration of the panoptic surveillance of Foucault (Danaher et al., 2000), in combination with the contributions of Marxist political economists on what is understood as informational capitalism, a paradigm in which the technology of knowledge generation becomes source of economic profit (Fuchs, 2010).

The idea of the Panopticon has been often used to describe the phenomenon of mass surveillance by law enforcement and intelligence agencies, often in connection with the Snowden Revelations (Horowitz, 2017). However, its value as a concept goes beyond the understanding of new forms of state power emerging from the diffusion of information technologies. Indeed, surveillance can take many forms, from workplace surveillance to CCTV, from data analytics for national security to advertisement purposes, which is the central focus of this thesis. Previous research on the topic outlined the necessity for conceptualizing the new social relations of production and surveillance enhanced by new technological developments and encapsulated in what is defined culturally as the Californian ideology, which stresses individualism, personal responsibility, competition, private property and consumerism (Fuchs, 2012). It is therefore necessary to adapt this conceptual framework to the specific case of the advertisement ecosystem and its ramifications in the political and social spheres.

In the interpretation of Foucault (Danaher et. al., 2000), the practice of surveillance occurs through what is defined as power-knowledge, understood as the disciplinary aspect of power, which is exemplified by the Panopticon. The Panopticon, in original Bentham's conception, was

[2] For example, Google-owned DoubleClick has the highest market share in this sector at 60% (Source: https://www.datanyze.com/market-share/ad-exchanges/doubleclick-market-share).
[3] A cookie is data sent from a website and stored on your computer which allows websites to record your browsing activity and remember information (Source: Collins Dictionary).

> "a tower placed in a central position within [a] prison. From this tower, the guards would be able to observe every cell ..., but it was designed in a way that the prisoners would never know whether they were being observed or not. Prisoners would assume that they could be observed at any moment and would adjust their behaviour accordingly." (p.53-54)

In this way, Foucault argues that surveillance significantly alters the human behaviour as it produces a culturally enforced disciplinary order. In the context of the internet, surveillance occurs through technologies of information gathering and analytics to reveal patterns and generate inferences on a particular group of internet users and their preferences, attitudes and more. As regards the wider internet ecosystem, Campbell and Carlson (2002) consider data collection and analytics by web giants as an effort to use surveillance technologies to manage consumers through techniques of advertisement targeting. This trend is consistent with a more general dynamic in which new information and communication technologies are now inserting themselves in the planning and controlling of the production process through data collection practices, including not only the managing of the workforce, but also consumers.

A noticeable difference from the original Foucauldian conceptualization of the Panopticon, as Campbell and Carlson claim (2002), is that in cyberspace, individuals actively cooperate in the online gathering of personal data about themselves in a dynamic defined as self-surveillance. Self-surveillance, in the case of internet services, is not cultivated through the threat of coercion, but though the threat of exclusion, or "losing out" (p. 594). In fact, as Hull (2015) claims, the choice to decline the participation in privacy-harming online services is becoming increasingly costly for the individual, from a social but also economic perspective. Indeed, the reality of behavioural tracking in the advertisement market can be understood as a "panopticon based on positive benefits" (Whitaker, 1999, p. 139). In the case of the free services provided by tech corporations such as Google or Facebook, users are compelled, in order to access these services, to give consent to the collection and processing of their data. This is part of a model known as privacy self-management, where users are regarded to evaluate their privacy choices through a rational cost-benefit evaluation. Arguably, such incentives towards data disclosure compel the individual to give away privacy in exchange for the positive benefits offered through services by those corporations. As Hull (2015) describes, the conception that privacy is an individual, commodified good that can be traded for other market goods represents, in Foucauldian terms, an instance of ethical subject formation in which privacy norms and practices are normatively constructed in a neoliberal direction.

The point of why users accept to participate in these mechanisms of surveillance represents an important intersection with Critical Theory and Marxist political economics. According to Fuchs (2012, p. 708), users are ideologically coerced to use commercial platforms in order to be able to engage in communication, sharing and the creation and maintenance of social relations, without which their lives would be less meaningful. In short, his main contention is that the ideological coercion lays in the threat to have less social contacts because of missing information from the media and missing communication capacities that are needed for sustaining social relations. This trend, according to Cohen (2008), reproduces patterns of asymmetrical power relations between workers and owners, including extensive commodification.

Furthermore, due to the ability of the supplier of the service to set the terms of the contract that the user can only accept or decline, the transaction is inherently inequitable. Indeed, the consumer is ultimately a "contract taker, rather than a contract maker, and thus provides the information in the belief that it represents a reasonable transaction cost." (Campbell & Carlson, 2002, p. 591). These perspectives shed critical light on the current understandings of online consent, which is rooted in the internet

ecosystem by providing the prevalent model for the "terms of use" of online services. In this context, the notion of informed consent and privacy self-management can be called into question for the flaws of their inherent assumptions.

What is meant by extensive commodification of the user? Again, critical perspectives on the topic allow for a conceptualization of the capital accumulation mechanisms on which major IT corporations base their business models (Hoegg et al.,2006). The contention of critical research on the topic is that users on these platforms are at the same time the consumers of the advertisements and the producers of the data on which the advertisement is based. This leads some authors (Fuchs, 2012; Rizer & Jurgenson, 2010; Terranova, 2000) to conclude that the user in the digital economy covers the function of a consumer-producer. In this context, economic surveillance on corporate platforms through data collection and analysis of user-generated content allows for a new capital accumulation model based on targeted advertisement and profiling. Indeed, according to Cohen (2008), by inputting detailed information about social and cultural tastes on platforms such as Google and Facebook, the producer-consumers generate immaterial labour, which is harvested by proprietary algorithms to generate capital accumulation and penetrative commodification.

The essence of this productive process brings forward another issue, that of the ownership of data, which has great implications on the conceptualization of user privacy. What generates the market power of these companies is the sheer amount of data they hold about a large part of the population using their services, through what Yoo (2011) describes as network effects, namely when the value of a network depends on the number of users connected to it. In this context, the larger the sample of users, the higher the value of the network, increasing also the accuracy of the data-mining techniques performed. This causes platforms to adopt strict consumer-retention policies which result in lock-in effects, i.e. when the data the user has "invested" in the network, such as messages, photos, reputation and search histories, remain within the original platform (Engels, 2016). This process arguably puts the user in a position of significant power asymmetry, where the preservation of privacy through the abandonment of a particular platform comes with high costs related to the loss of the social capital they invested in the network. Therefore, it is possible to claim that data ownership is of crucial importance for the understanding of the political economy of surveillance, touching upon the monopolistic character of Web 2.0 platforms which prevents users from being owners of the data they produce and which prevents them from enabling privacy self-protection measures, such as transferring their data to alternative, privacy-conscious networks.

The last and intrinsic element of the political economy of surveillance is the nature of profiling. Profiling, according to Clarke (1993), is "a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and dataholdings are then searched for individuals with a close fit to that set of characteristics." (p. 405). In the advertising ecosystem, profiling represents the primary source of profit as it allows personalized customer relationship marketing to provide tailored content (Turow & Draper, 2012, p. 139). However, some profiling practices can cause negative consequences on individuals and society at large. Such risks encompass discrimination, inequality, stereotyping and inaccuracy of the decision-making process (Gare, 2016). Indeed, as Lyon (2008) reports, consumer surveillance using database marketing produces discriminatory practices that "cream off some and cut off others" (p. 1), in a practice described as "social sorting", which can also be applied to smart policing techniques.

The issue here, is that the panoptic sort does not only profile users in order to acquire insights on

their patterns of behaviour, but also acts on the basis of these patterns through automated decisions which produce an effect on the consumer. These automated decisions based on online profiles, from the perspective of surveillance studies, bring forward the issue of how algorithms take decisions on real persons on the basis of the information they hold on them, often providing new insights but also engendering new risks. Algorithmic decision making, in this case, refers to the capacity of providers to perform automated decisions on a subject based on the profiling practice conducted on him/her, the accuracy of which can be contested (Ratti & Helbing, 2016). For instance, placement of a tailored advertisement based on browsing history does not have the same effect on users as the raising of insurance value based on the analysis of consumer behaviour in the Internet. Although both cases can be based on profiling, the effects are substantially different (Gare, 2016).

In conclusion, the observable dynamics of profiling techniques can be summarized as intrinsic characteristics of a political economy of surveillance, in which the producer-consumer consents to these data collection practices through ideological coercion. At the same time, the consumer is the recipient of decisions taken on the basis of the data produced, the logic of which is not allowed to be known due to intellectual property regimes (Cohen, 2008). Therefore, as concerns the issue of profiling, it is possible to argue that the lack of transparency and accountability for automated decision-making mechanisms is a characteristic of this economic model, which enhances the potential for inequitable power-relations.

The proposed framework of a political economy of surveillance therefore provides a conceptual depiction of the business practices of some of the major Web 2.0 platforms such as Google and Facebook; practices that have become topics of debate in the academic and political spheres, due to large pools of users of these platforms and the sheer power that derives from it. Firstly, IT corporations coerce users to accept surveillance practices in exchange for the use of a service using the threat of exclusion from the social and economic benefits correlated with the platform use. These practices therefore create a problem which concerns the mechanism of online consent. Secondly, users cover the function of producers-consumers, in a model of capital accumulation which is based on the harvesting of "immaterial labour" through proprietary algorithms. This matter is connected with the ownership of the data, as these quasi-monopolistic web giants adopt strict consumer retention policies which create a lock-in effect on users.

Thirdly, once the mechanisms of data collection and retention have been clarified, it is important to denote the logic on which the act of profiling is based, namely algorithmic data-mining and automated decision-making mechanisms, which engender wider societal risks including the reinforcement of discriminatory practices and inequality through a process of "social sorting". The functioning of these algorithms presents a fundamental question of transparency, as these machine-learning techniques produce real effects on users' lives. In conclusion, measuring the influence of this model on normative conceptualizations of the Internet is a compelling task for critical research on this topic, and ought to be aimed at the deconstruction of these norms in their political and social dimensions, in order to understand how they are reproduced by everyday practices, as in Foucauldian governmentality (Berenskoetter, 2016). Certainly, one of the most prominent of these dimensions is that of policy, which will be addressed in the next chapters through a case study of the General Data Protection Regulation.

3. Analytical Framework

As this paper attempts to generate a comprehensive theoretical account of the dynamics of internet surveillance embedded in the business model of major IT corporations, the analysis takes the form of a theory testing academic enterprise. The analytical approach identified for this research is to account for

public value systems, configuration of knowledge into a mode of governance, which has the potential to reflect the core concepts on which the thesis is based. This research enterprise therefore occurs at the intersection of political philosophy, sociology and political science, with a focus on the transformational effects of digital technologies and neoliberal capitalist development. Indeed, as Berenstkoetter (2016) reports in his account of the Foucauldian tradition of conceptual analysis, it is possible to explore how instances of knowledge production, in this case a regulation, highlight power-structures that emerge out of and are reproduced by everyday practices.

The purpose of the analysis is to bring to the fore the normative paradigm from which the Regulation originates, through a process of deconstruction and reconstruction, in order to highlight how the identified concept mirrors governmental practice. As Schulze (2015) describes in his account of surveillance legitimation in Germany, power-relations originate from different normative paradigms, which can be empirically identified and deconstructed for the purpose of critical research. On this basis, the case of the GDPR, due to its highly contested nature (Financial Times, 2018), provides the opportunity to trace the normative stance underpinning the legal instrument through an abundance of secondary legal literature. Therefore, in order to connect the theoretical tools provided by the political economy of surveillance with the selected empirical base, this thesis details in the three following subsections the analytical framework adopted for the identified concepts: consent, data ownership, and profiling. Lastly, this section provides an overview of the methodological assumptions and relevant limitations, together with an account of the relevance of the chosen case.

3.1. Consent

The issue of consent, which regulates the relation between producer-consumer and company, is regulated by Recital 25, Recital 34, and Article 7 (European Union, 2016), and is assessed through the lens of the criticisms to the informed choice model. Consent here ultimately refers to the power asymmetry between the company and the user, and thus, the operationalization of this concept follows the level of control that the user has on data disclosure. According to Carolan (2016), this mechanism is currently rooted in the behavioural science practices aimed to intuitively impel the giving of consent thanks to the architectural discretion that these companies enjoy. In this sense, we can distinguish between an "opt-out" and an "opt-in model" (Fuchs, 2013, p. 63). An opt-out model assumes that the user (data subject) wishes to exchange his privacy for a service in a mechanism of "voluntary exchange", while an opt-in model assumes that the subject does not wish to disclose personal data and may only wish to do so if he consciously wants to join the ecosystem of profiling. In the middle, it is possible to encounter normative prescriptions which are based on an opt-out model but acknowledge the significant power asymmetry between the user and the provider, for instance, by requesting the provider to give sufficient information before consent is given or by limiting consent as a valid ground in certain specific cases. The analysis of consent therefore follows this operationalization in an attempt to detect on which side of the opt-out and opt-in spectrum the Regulation is normatively conceived.

3.2. Data Ownership

The issue of data ownership ultimately refers to the extent to which the data subject is in control of the data she/he produces. Consequently, this section operationalises this concept by relating it to the Right to be Forgotten and the Right to Data Portability, two gradually established principles originating in the

implementation of Article 12 of Directive 95/46/EC, which consist of the right of the user to demand the erasure of all her/his personal data held by the service provider, as well as the possibility to access personal data when stored in a processor's systems (Mantelero, 2013). These rights are regulated by Article 17 and Article 20 of the GDPR (European Union, 2016). These measures are important for their relation to the quasi-monopolistic stance of major IT corporations, as they allow users to easily switch between competing service providers and requesting the erasure of all personal data held by the processor, relating ultimately to the philosophical aspect of the ownership of data.

In this case, the analysis assesses to which extent these articles establish a normative prescription that allows users to take back control of their data, by facilitating data migration to other platforms (with different privacy standards) or by requesting the erasure of such data in its entirety. As these rights were already established through the interpretation of previous legislation on the issue, the concept of data ownership is operationalised in a dichotomic "partially exercisable" and "fully exercisable". Potential limitations to this right encompass cases where the service provider is allowed to retain relevant information on the subject despite the user's request, or where the user is compelled to provide legitimate grounds for the erasure or the access. In practice, these rights might be limited in a way where a substantial part of personal data will remain untouched, or the monopolistic character of these companies would not be threatened, therefore legitimizing a political economy of surveillance. On the opposite side, a fully exercisable set of rights would potentially threaten the monopolistic character of those business models, due to the change they would cause to the normative context in which they operate.

3.3. Profiling

Lastly, the analysis encompasses the issue of profiling, which deals with automated decision making on the basis of user characteristics detected in the data processing process, which is dealt with by Recitals 51, 58, 59 and Articles 21-22 (European Union, 2016). Here, this measure is particularly relevant for the overall reflection of a political economy of surveillance, as profiling represents the major source of profit of Web 2.0 giants. Furthermore, the fact that profiling is specifically acknowledged and regulated through this instrument brings forward the issue of how much this practice is legitimized. The main approach here is to operationalize this concept by looking firstly at the extent to which users can object to profiling and secondly at the extent to which they can receive precise information about the nature of an automated decision concerning them, with clear limits on the types personal data on which the profiling can be based. These conditions would arguably allow the data subject to opt-out of behavioural advertising mechanisms, as well as preventing discrimination based on factors such as income or race to be carried out through automated decision making (Gare, 2016). A situation where both conditions will be met will be considered as "restricted profiling", while a situation where only the latter applies will be considered as "partially intrusive profiling", as users will only be informed and will not be able to opt-out from behavioural targeting. Ultimately, a situation where none of these conditions apply will be "intrusive profiling".

3.4. Methodology

The analysis performed in this thesis consists of an exploratory research, as the primary aim is to explore what can be learnt from the conceptualization of a phenomenon in a particular case. This research has a qualitative nature, based on post-modernist and post-structuralist epistemological assumptions (Hesse-Biber & Leavy, 2011, p. 21-22). In this context, post-modernist and post-structuralist assumptions allow for a measurement of underlying normative stances that are reproduced in the social environment and

produce power-relations. By employing this set of assumptions, the analysis focuses on the normative implications of the primary text, addressing it from a critical perspective in light of the established framework and interpreting it through relevant secondary literature. Furthermore, in accordance with Toshkov (2016) the present paper selects types of indicators that "are indirect and usually do not allow for a precise measurement, but only for detecting presence or absence in a rough-and-ready way. When there is no direct correspondence between the concept and the observable indicator used to detect and measure it, operationalization provides for indirect proxies" (p. 101). In this context, the operationalization of the relevant concepts occurs mainly through arbitrary categorizations, which aim to reflect the various degrees of applicability of the theoretical framework to the empirical base.

Therefore, there are several potential limitations in the chosen methodological approach, most prominently the fact that policy outcomes are often the result of complex political compromises, which are both difficult to evaluate and systematize into one value-structure (Sevenhuijsen, 2004), which is particularly the case for the final version of a highly contested regulation. Therefore, the necessity for a further layer of abstraction has the potential to limit the reliability of the detection of the underlying philosophical and normative components. Furthermore, as Cohen (2015) claims, academic work in surveillance studies so far has not been well adapted methodologically to the study of the evolution of policy responses to commercial surveillance. This arguably causes a "black-boxing" of the legal processes, which are sites of contestation over modalities and limits of surveillance. On the other hand, legal scholarship on privacy and data protection often overlooks the way surveillance practices shape subjectivity, culture and power. In this context, this paper acknowledges such lack of methodological integration and aims to build a mode of inquiry in this direction. Moreover, this paper aims to compensate limitations in the analysis of primary data by employing a vast available amount of secondary literature on the issue, where the connection between specific measures and their normative implications are highlighted. Annex I outlines a wider acknowledgment of this paper's limitations.

3.5. Case Selection

In order to discuss the presence of a political economy of surveillance in the European context, this paper performs a case study of the final version of the General Data Protection Regulation (European Union, 2016), as it represents a major policy initiative directed at regulating the cyberspace. In fact, as Buttarelli (2016) claims, the EU GDPR raises the bar for data protection laws around the world, representing a step forward towards a "digital gold standard" (p. 78), in which a common set of norms governing data protection practices would be widely recognized and applied. Furthermore, the domain of the Common Digital Market is a recent appearance in the EU policy debate, which renders the critical analysis of the Regulation important in order to understand the underlying normative structures that prevailed in the formulation of this policy instrument. Indeed, according to Regan (2012), the available regulatory approaches towards surveillance technologies are developed along different traditions, varying from case to case according to factors such as political culture and system of government. In the US for instance, self-regulatory arrangements by the industry are preferred, which rely on tools such as due-diligence and self-certification. In Europe, instead, the prevalent approach is national governments regulation, which relies primarily on regulatory authorities and the judicial branch for the implementation of regulations (p. 403). As the GDPR represents a step forward in this regulatory practice, namely the harmonization of data protection rules at the supranational level, it is crucial to critically address the normative drivers of

regulation in this particular field.

It is therefore possible to consider the GDPR as a potential empirical testing ground for the political economy of surveillance. The proposed case study does not attempt, however, to conduct a policy analysis, but it aims to evaluate to which extent the Regulation reflects this political-economic framework. It therefore does not address specific features of the European policy process, nor attribute a specific normative stance to particular EU institutions. Indeed, outcomes of EU policy processes are result of political compromises and legal-technical considerations, which require specific theoretical and methodological approaches. The present study addresses solely to which extent the practices identified in the political economy of surveillance are legitimized or constrained by this piece of legislation. More specifically, how the phenomenon described by the theory is reflected in policy practice, in its underlying normative stance. In fact, according to Zarsky (2016), the GDPR is premised in "deep philosophical convictions regarding the extent to which specific rights of both individuals and groups must be protected in the digital age" (p. 997). Consequently, the case of the GDPR is adopted in order to deconstruct these philosophical assumptions and to assess the extent to which they reflect the abovementioned concept, due to the relevance of this policy instrument in regulating the domain of cyberspace in a context of an increasingly connected society.

4. Analysis: Case study of the General Data Protection Regulation

4.1. Consent in the GDPR

Consent occupies a prominent role in the regulatory framework established by the GDPR. In this context, it is important to highlight the definition provided by Recital 32 (European Union, 2016), which states that "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data". Arguably, this choice would imply a move away from the assumptions of passive consent, by conceptualizing it as an act that should be freely given and informed. Indeed, the recitals proceed by detailing that "silence, pre-ticked boxes or inactivity should not therefore constitute consent." Indeed, as Carolan (2016) claims, the inclusion of this statement indicates a move towards a model of active consent, where the conferral of authorization for data processing is based on a clear, informed and affirmative action by the user. However, as the author also denotes, Recital 32 includes the possibility for data controllers to include "pre-formulated" declarations of consent as long as they are provided in an intelligible form, implying a reluctance in requiring direct and active engagement by the user. This limitation is particularly relevant as online service providers possess significant creative control over their architectural choices, which has consequences on the informational self-determination of the data subject. Consequently, by employing behavioural science models (Acquisti, 2009), providers are able to circumvent such requirements by designing interfaces which intuitively compel the user to provide his/her consent.

It would be possible to argue that within the identified analytical spectrum, the Regulation implies a normative understanding of consent which is based on a mixture of opt-in and opt-out features where its opt-out character is more demarcated, reflecting partially the identified dynamic of the political economy of surveillance. Indeed, while the move from a passive to an informed and active consent implies a normative shift towards greater informational self-determination, the prevalence of a doctrine of "informed consent" represents a legitimation of the asymmetrical power relation between the user and the provider, which is ultimately detrimental to user control. Indeed, as Acquisti (2009) claims, behavioural economists design systems to "nudge" individuals, sometimes exploiting the very fallacies and biases they

uncover, turning them around in ways that diminish users' freedom and preclude the possibility of an informed choice. This is especially the case in the way the Regulation has been conceived, which does not provide, according to Carolan (2016), sufficient guarantees for user control in the process of data disclosure, and does not acknowledge the use of "nudging" nor situations where the user is in a position of dependence from the provider. According to him, relying on a model of informed consent has been rendered ineffective by such technological developments in surveillance. It would be therefore possible to claim that the trend of a political economy of surveillance applies to the conceptualization of consent inscribed in the GDPR. The relevance of these findings therefore lays in the need to conceptualize new forms of online user-provider relations that would further enhance informational self-determination in contrast with a model of privacy self-management inscribed in the practices of major IT corporations and, as demonstrated, in the normative component of policy practice.

4.2. Data Ownership in the GDPR

Regarding the issues of data ownership, the Regulation takes a more proactive stance in its conceptualization of user control of personal data. In this sense, the Right to be Forgotten represents the first expression of this stance, which is based on the decision of the European Court of Justice in the Google-Spain case (De Hert & Papakonstantinou, 2012) and a strong consensus within the Article 29 Data Protection Working Party (2012), a Commission-established advisory body. In this sense, the Right to be Forgotten as established in Article 17 (European Union, 2016) prescribes that users should be allowed to have the processor erasing all personal data concerning them under a series of conditions, including when the user withdraws consent, when personal data has been unlawfully processed as well as other instances. In this current formulation, the Right to be Forgotten effectively implies a normative stance which attributes significant control over the erasure of personal data to the user (Mantelero, 2013). In fact, apart from limitations concerning freedom of expression and information, which are beyond the scope of this analysis, it is possible to argue that in regard to erasure, data ownership is being conceived as fully exercisable.

The Right to Data Portability, in comparison with the Right to be Forgotten, is much more of a recent introduction. The novelty of this article lays in the possibility to obtain a copy of personal data held in a processor's systems in a "structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance" (European Union, 2016). This norm has a significant role in relation to the monopolistic stance of major IT corporations and its application could trigger easier migration of users from platform to platform. Indeed, Koops (2014) argues, the choice of framing data portability essentially as a data protection measure, although such a regulatory intervention is more attributable to issues of competition law, signifies a normative stance that acknowledges the significant lock-in practices of major providers. In this context, the right to data portability can be considered as fully exercisable and does not consequently reflect the current conceptualization of a political economy of surveillance.

A potential explanation might reside in the normative context in which these providers have developed, the previously described Californian ideology (Fuchs, 2012), and its differences from the European one. Indeed, it could be possible to explain this deviation from the model of political economy of surveillance as a point of differentiation between the tradition of "ordoliberal" antitrust legislation originating in Europe, which sustains more distributed markets to foster competition, and a neoliberal

tradition in which monopoly power can be a considered as a reward for efficiency (Van Horn, 2009). It is therefore possible to argue that this normative stance represents a deviation from the described characteristic of the political economy of surveillance, due to the overlap of social norms on data protection with competition principles embedded in European regulatory traditions. The relevance of such finding is that these traditions will also impact the norms of the internet environment, highlighting the need to adapt the focus of analysis of the political economy of surveillance to different normative contexts, such as the European policy one. Furthermore, from a critical perspective, such stance has the potential to generate an opening that could lead to the growth of alternatives to the dominant business models, enhancing the emancipatory character of the internet.

4.3. Profiling in the GDPR

Profiling is widely regarded as being a practice that carries more risks the more it becomes entrenched with everyday lives of citizens and shape their interactions with institutions and market actors. According to Article 21 of the Regulation, users should have the right to object to their personal data being processed by a controller (European Union, 2016). Furthermore, Article 22 expresses that the data subject shall "have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her". The interpretation of these two measures is contested, as it is not clarified to which circumstances the condition of "significantly affects" would apply (Gare, 2016). However, as it can be noted in the interpretation provided by De Hert and Papakonstntinou (2016), the Regulation adopted the point of view that the merits of profiling outweigh its disadvantages and regulatory control can mitigate risks while maintaining a permissive attitude towards the phenomenon.

As Koops (2014) points out, this aspect of the Regulation is conceived not only to restrict, but also to enable the free flow of personal data by bringing the profiling industry under a common framework to facilitate business. In this context, if the price of a health insurance would be raised based on online profiling, such practice would be conceptualized as discriminatory. However, the larger systemic dynamics would be left untouched by the Regulation, as requirements to explain the logic behind algorithmic decision making are hampered by the intellectual property character of those algorithms and the extent to which individuals can be considered as significantly affected has limited applications in practice (Zarsky, 2016).

It is therefore possible to claim that in this context, the normative stance on profiling that is detected is one of "restricted profiling", in which major discriminatory practices are excluded but the current profiling practices in the domain of the advertising ecosystem are essentially legitimized. The attribution of the normative component of the Regulation in this regard as "restricted profiling" is therefore relevant as it established a conceptualization of the political economy of surveillance in which major risks are acknowledged but common practices of profiling are indeed legitimized. As the value of personal data of EU citizens is forecasted to reach one trillion euros by 2020 (European Commission, 2017), these findings highlight the need to conceptualize the profiling practices of the advertising ecosystem by taking into account not only major risks, but diffused trends which perpetuate asymmetrical power relations on the internet, such as intrusive commodification of consumers.

5. Conclusion

The present critical study examined the extent to which the proposed theoretical perspective of a political economy of surveillance applies to the case of the EU General Data Protection Regulation. By drawing from relevant literature in surveillance studies, critical theory and Marxist political economics, this thesis has

tested how the phenomenon identified by the theory reflects the underlying normative stance of the Regulation. The findings highlighted the applicability of the current conceptualization of the political economy of surveillance to two out of the three identified topics. Firstly, the analysis showed how the regulation adopted a normative model of "informed consent", reflecting the assumption of voluntarism embedded in privacy-self management that perpetuates asymmetrical power-relation between users and providers. Secondly, the study revealed how the concept of data ownership has been translated into policy practice in a way that does not reflect the framework of a political economy of surveillance, due to the normative divergence between an "ordoliberal" regulatory tradition and the neoliberal model from which these practices of surveillance originate. Thirdly and lastly, the inquiry conducted on the aspect of profiling highlighted how the normative stance of the GDPR legitimizes the current dynamics of profiling in the advertisement ecosystem, while also aiming to restrict its most discriminatory practices. In conclusion, it is possible to argue that in the areas of consent and profiling the GDPR reflects a political economy of surveillance, while a noticeable divergence in values was encountered for the aspect of data ownership.

These findings indicate the relevance of this multidisciplinary theoretical perspective in the study of the transformational effects of digital technologies and neoliberal development, and their effects on the regulation of cyberspace. By performing a case study of the GDPR, the present thesis aimed to contribute to the body of academic literature in the field of critical and surveillance studies by providing an account of the underlying value-structure of this regulation. Limitations to the study include the difficulty in systematizing policy outcomes in a single set of normative assumptions, since they are influenced by a variety of factors involving political compromises and legal considerations. Consequently, the study aimed to supplant the risk of such methodological black-boxing of legal processes by employing relevant secondary literature which allowed for a clearer categorization of the normative components of the GDPR.

The empirical patterns identified in this thesis shed critical light on the current trends in information technologies by accounting for the replication of neoliberal modes of development in the domain of internet. In the European case, it is possible to notice that this mode of development is culturally replicated in its core components, excluding the area of data ownership and monopoly power where the European regulatory traditions diverge from the normative context in which major IT corporations originated. The relevance of this divergence lays in the possibility for a structural change in the norms governing social interactions on cyberspace, towards a direction where alternatives to the prevalent models can emerge.

More broadly, this thesis highlights the need to further develop critical conceptual toolkits to evaluate the transformational effects of surveillance technologies and provide for normative and political alternatives to enhance informational self-determination and emancipatory practices in this domain. For instance, further research on the topic could be conducted by employing the current framework of a political economy of surveillance to evaluate, through a critical discourse analysis, how issues of privacy and data protection are framed in the media in connection with the recent scandals such as the Cambridge Analytica case or the entrance into force of the GDPR. Overall, it is possible to claim that in the context of the increasing relevance of information technologies in our daily lives, there is the need to further untangle the dynamics of current intrusive surveillance practices and their reflections in the social and political domains. In particular, for those of us who grew up in the internet environment and saw a shift from a free and open institution that enhanced collective creation and dissemination of knowledge, to a privatized space where intrusive surveillance is ubiquitous, this represents a compelling task for the years to come.

6. Annex I

Acknowledgements

General premise: This paper touches upon technical issues related to information technologies from a strictly political and philosophical perspective. Consequently, this approach might lead to the oversimplification of technical issues that are debated in sector-specific forums since many years. The author of this paper is aware of those debates and attempted to take into account these perspectives and sensibilities by receiving technical advice from developers and programmers. However, the author apologizes in advance to the community for the technical inaccuracies expressed for reasons of conciseness.

Not Specific, but General Data Protection Regulation: This paper acknowledges that the GRPR has been developed to encompass a wide range of practices of data collection and processing, which are not limited to Silicon Valley giants but range from scientific research to the provision of public services; from small and medium enterprises to banks, ISPs and credit rating agencies.

Metadata: The issue of whether metadata can be considered as personal data has not been addressed conceptually in this paper. For a matter of clarity, this paper adopts the standpoint of considering metadata as undoubtedly personal data. More info can be found at https://www.eff.org/search/site/metadata

Right to Data Portability: This paper acknowledges the technical controversies around this particular right. Indeed, the interoperability of the data is a highly technical issue, with the problem of which format should be used to provide personal data back to the user (especially for metadata). The paper therefore does not assess technical issues related to interoperability but focuses on the existence and scope of the right alone.

Profiling: The considerations detailed in the section on profiling are based on the assumptions that algorithms can reinforce and reproduce human bias.