Beyond the commodification of privacy: Personal data management as a strategy for accountability in a digital world

Jaseff Raziel Yauri Miranda[1]

Abstract

This theoretical article questions to what extent digital flows are articulated to enhance accountability within democratic paths. The aim is to analyze accountability principles across legal frameworks (institutional dimensions), market practices and societal strategies (functional dimensions) at European level. We are focused on the management of personal data in a digital world because data fragments could be deemed as extensions of physical bodies and traditional biopolitics. The article is structured to analyze the cross-references and influences within the triangle state-market-society. This structure apprehends the connections, representations and the limits of accountability regarding personal data. The conclusion summarizes those limits and distinguishes essentialist and deterministic approaches of digital networks as automatic enhancers of accountability principles.

Keywords: accountability, internet studies, digital politics, personal data, privacy, commodification, surveillance

Resumen:

Este artículo teórico cuestiona hasta qué punto flujos de información digital se articulan para promover principios de accountability dentro de caminos democráticos. Para ello, se considera la administración de la accountability dentro de marcos legales (dimensión institucional) y en las estrategias empleadas por actores del mercado y societales (dimensión funcional) a nivel europeo. El enfoque recae sobre el uso de datos personales como trasfondo del mundo digital ya que esos pueden ser considerados extensiones de cuerpos físicos y de la biopolítica tradicional. El artículo está estructurado para analizar interrelaciones e influencias dentro del triangulo estado-mercado-sociedad. Esta estructura aprehende las conexiones, representaciones y límites de la accountability para crear y procesar flujos digitales. La conclusión sintetiza esos límites y distingue posiciones esencialistas y deterministas sobre las redes digitales como promotores mecanicistas de accountability dentro de principios democráticos.

Palabras clave: accountability, internet, políticas informacionales, datos personales, privacidad, vigilancia.

[1] Ph.D. student in Society, Politics and Culture at the University of the Basque Country (UPV-EHU). Master degree in Governance and Political Studies (UPV-EHU) and Degree in History with complements in Political Science at the Federal University of Minas Gerais (UFMG), Brazil. He was a member of the "Center for Strategic Studies and Intelligence" (CEEIG-UFMG), coordinator of the "International Law and Governance" research committee in the "International Association for Political Science Students" (IAPSS), and reviewer in several international political journals. This paper was funded by the Predoctoral Research Program from the Basque Education Office.

Introduction

Since the creation of the first Internet networks, some foresaw the widespread adoption of computer technologies as human redeemers. In 1978 Roxanne Hiltz and Murray Turoff, in "The Network Nation", believed that networking would promote gender equality and speculated that electronic discussion and voting would revivify the public sphere in democratic societies. During the 90s, digital networking was a change comparable in significance to the Industrial Revolution transforming every aspect of our daily lives (Castells, 2011). Even official briefs believed that the "informational era" enabled the creation of perfect public spheres, the Agora of Ancient Greece, a meeting place with no intermediary, exercising all their political rights unconditionally and without restriction (European Information Society Forum Report, 1999).

By those years, critical democracy seekers, instead, expressed that such management and digital potentials excluded voices in such a way as to directly challenge existing institutions. In that sense, online and offline democratization procedures were apprehended in a dichotomy between institutional powers and civil agency energies. For instance, the institutionalization of web democratic action was deemed as an attempt to tame radical energy from society (Blaug, 2002). However, we argue that a normative regulatory effort could complement and be complemented by democracy seekers and e-democratic counter-publics. That is, institutional and functional dimensions are not exclusionary to strengthen democratic principles such as accountability.

This nuanced position tries to avoid the perception that the World Wide Web only reinforces the status quo' (Margolis and Resnick, 2000). Some critics go as far as to argue that, rather than invigorating it, the Internet could seriously undermine the health of democracy, by providing access to individualized information environments resulting in group polarization, by forcing political arguments that become "distorted, shrill, and simplistic" amongst the array of competing online messages (Noam, 2002). While we reject utopian and dystopian ideas that followed the 90s rhetoric of internet triumphalism, it does not mean that we ignore the increasing dispute and expansion of institutional and especially commercial forces. These have occupied the Internet to dominate what was never a sacred open domain. What is more, Shanti Kalathil and Tyler Boas (2003) demonstrated that closed regimes have learned how to stifle the bottom-up democratic potential of the Internet and we have seen this after the Arab Spring during the last decade. Moreover, the Huxlian idea that new communication technologies such as the Internet tend to distract more than empowering citizens must be considered seriously even if it is not an absolute condition adopted by Internet users.

As digital flows change our daily interactions and redefine our political preferences, it is arguable that institutions of marketing and older bureaucracies have become malleable. Indeed they modulate the control inferred by Gilles Deleuze (1995) in his work on the "society of control". For instance, surveillance tools have expanded their range and have become multifaceted for distinct purposes. The use of software and statistics to socially sort all manner of populations has now become a base mode of organization in almost any enterprise, public or private (Beer and Burrows, 2010).

Hence, analyses of those who apprehended the interactive, participatory and voluntary empowerment capacity deployed by the web 2.0., have been shadowed by bedevils behind the social network. For Mark Andrejevic, internet and social media users are an "audience commodity" sold to advertisers. The fact that they are also content producers mean not that media is thus being democratized, but rather that this is the advent of "total commodification" of human creativity (Andrejevic, 2011). The broader the extension of business and government interests on the web during the last decades, the broader has been the capacity to spread the commodification of privacy and surveillance activities that emulate the offline world. For instance, we face "surveillance assemblages that operate by abstracting human bodies from their territorial settings, separating them into a series of discrete flows (…). The surveillance assemblage transforms the purposes of surveillance and the institution of privacy" (Haggerty and Ericsson, 2000: 605). In that sense, digital footprints and personal data are extensions of biopolitics in liquid assemblages. Thus, a question of legitimacy arises: who is responsible for this translation of information and who takes responsibility for the data usage? Usually, state forms would be held responsible for the deployment of biopolitics over individuals. But as the digital world is not disconnected from a physical one, the challenge also consists in turn responsible and oversight extra and para-state players whose functionalities and political strategies are crucial to the contemporary governance.

Operationalization

As starting points, we question to what extent we should think of digital flows as a potential space for the articulation of accountability within a deep democratic action. And how are citizens reacting beyond institutional and market spheres to influence data usage and those who govern them? In light of these questions, the aim of this article is to analyze accountability principles within legal frameworks (institutional dimensions) and in those strategies deployed by the market and societal players (functional dimensions beyond institutions). Despite being a catch-all term, accountability is appropriated and transformed by this triangle (state, market, and societal players) in a cross-referential influence with specific interests. We consider the use of personal information as a background in a digital world because data fragments could be deemed as extensions of physical bodies and traditional biopolitics. It is of interest to apprehend the connections, representations and the value given to accountability when it comes to creating, sorting and processing digital flows. These intersections, among accountability and digital flows, could help us to improve the understanding and redefinition of social and political asymmetries which are permeated by technological tools and informational networks.

As introduced before, we distinguish our position both from essentialist and deterministic accounts of the virtual networks as mechanic enhancers of democratic and accountability principles. This article adopts a qualitative analysis of the attempts to improve accountability goals in a digital world. In that sense, it is of importance to

analyze shared norms and strategies, either at the core of institutions or beyond them. This approach avoids narratives that the Internet must become a preeminent space for institutional regulation which downplays the civil agency and vice versa. Therefore, accountability practices could be analyzed at the normative or judicial level and across the market and societal actions that are entangled to a social and constructivist perspective about the use of technology. This endeavor is not an exhaustive theoretical interpretation about democracy and democratic processes in digital flows. But as argued by Stephen Coleman and Jay Blumler (2009) some crucial lines could be deemed as starting points in every democratic effort. Those principles are a) regular, free and fair elections, involving competition between more than one party, b) The rule of law, under which all citizens are subject to a common jurisdiction, c) Freedom to speak, assemble and publish, and for opposition to the government of the day to organize without fear of intimidation, d) Government accountability to the public and responsiveness to public concerns, e) The existence of a civil society sector which is free from control by either the state or the market.

We have deliberatively chosen the accountability principle as it can be analyzed in a digital environment and in an array of political spheres from institutional to functional dimensions. This relates to the fact that accountability efforts must be expressed not only in legal terms but also by different social practices, functions, and strategies, even from those located at the margins of state and market spheres. Those relations are differently understood by scholars of behavioral, liberal, deliberative or agonistic democracy. The point here is to bring a theoretical analysis related to accountability within democratic lines, and data usage, especially when the data is collected from individuals. Ultimately, accountability goes further than the mere use of information and privacy as it means the creation of power and political intentions from different players in our contemporary world.

The accountability classic definition is related to answerability and enforcement. As stated by Andreas Schedler (1999), answerability is related to the capacity and prompt response of those political players that are held to justify and legitimize their actions. It makes “the accountable and accounting actors engage in a public debate in the light of the public interest” (Schedler, 1999:15). Enforcement is a call for punishment of the accountant actor after deviations of resources, information or power. It is understood as a stronger mechanism of accountability. Nevertheless, the “simple act of requesting information in the light of the public interest and the act of demanding responsible justifications for decision making” are mechanisms of accountability as well (Schedler, 1999: 17). Meanwhile, Guillermo O'Donnell (apud. Schedler, 1999) gives a distinction between horizontal and vertical accountability. In short, the former is related to a relation of equals in a chain of power or between institutions, such as the checks and balances and the delegated democracy principle. The latter refers to promote accountability in a locus marked by asymmetries of power, for instance, when superior ranks account lower officials in a hierarchical organization, or when the civil society ask for justifications of legislators in a context of a decision making.

This article analyzes accountability practices in light of the two dimensions expressed by Schedler and by appealing to O'Donnell horizontal and vertical relations. These concepts are basic for further definitions. For instance, as stated by Charles Raab (2013: 46), "institutions ought to be accountable to the governed, to those whose information they handle and to others who may be affected by such practices". Moreover, accountability definitions can evolve to external and independent controllers or to internal monitoring and regulators (Gray et al., 1996), either in horizontal or in vertical directions. Meanwhile, answerability can protect privacy and discourage unnecessary purposes with disproportional methods to sort personal data on the web. Thus, accountability, from a functional perspective, virtually provides the reversal from a method of control over citizens even in a context of hegemony as in the case of surveillance networks (Lyon, 2007). To summarize, accountability has the potential to be analyzed according to answerability and enforcement mechanisms in order to set parameters for the use of personal information inside democratic bases.

Despite the theoretical approach, we consider the intersection produced in the triangle state-market-society at the European Level. This level is the ground upon we analyze the accountability management. The first part of the article depicts and analyses how accountability principles are regulated in terms of Personal Data Protection in the European Union. This part represents the institutional dimension and the state-rooted accountability legal limits to collect and process individuals' information. The second part exposes how the accountability management efforts have been assumed by market players to implement institutional and state reforms. This part also analyses the limits of this new market approach and some key aspects such as Privacy by Design. The third part expresses parallel actions conducted by the social agency, such as hacktivism and online democracy seekers, exposing their strategies and weaknesses. Both the second and third parts privilege functionality dimensions for accountability and personal data. Our goal here is not to create a paramount conception about the mentioned strategies and players. Rather, the aim is to bring intersections and different accountability perspectives that can promote democratic paths, even if those paths are dispersed or represent distant political preferences.

1. Personal Data regulation

As the digitalization of information is ubiquitous, it was essential to create norms to handle and process sensitive individuals' information. At first glance, personal data could be irrelevant. Yet these data can be combined, fragmented and jointed to create an array of knowledge related to individual's political ideology, religious beliefs, and sexual preferences. Ultimately, a misuse or a deliberate edition of these data could result in harassment, social pressures, violence or even put some people at a disadvantage in their everyday life. Therefore, informational data management goes further than privacy as it is closely related to economic opportunities, surveillance of suspects and social interactions in a plethora of forms.

In light of the above, the Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) recognizes the protection of personal data as an essential right. It mentions that,

> Everyone has the right to protection of personal data, such data must be processed fairly for specified purposes and on the basis of the consent of the person evolved or for some other legitimate basis under provided by law, and everyone has the right to access the data collected relating to him/her and to get it corrected. (…) compliance with these rules shall be subject to control by an independent authority.[2]

Moreover, the European Parliament has produced several legislations on this matter. The Directive 95/46/EC is essential to regulate the procedures and transfers of personal data. Other examples are the Directive 2002/58/EC on the protection of privacy and data in electronic communications; and the Regulation (EC) 45/2001, which allowed the creation of the "European Data Protection Supervisor" (EDPS) as the Data Protection Authority (DPA). The DPAs have consultation and cooperation roles and support organizations across the Union to perform their obligations in terms of data protection. The Decision 2008/977 (Council on Justice and Interior Affairs) also regulates the protection of personal data in the context of police and judicial cooperation as well as in terms of Criminal Law. The Decision regulates data protection similarly to the previous "third pillar" of the Union and it is only applied to police and judicial data exchanges between the Member States, authorities, and systems of the UE (with no inclusion of national data bases). In the "Area of Freedom, Security and Justice" (AFSJ) –which is one front of the EU regarding security and surveillance practices- the main digital flows or systems across borders are the Schengen Information System (SIS_), the Customs Information System (SIA), the Information Visas System (VIS) and the European Police Agency (EUROPOL).

By those jurisdictions, State Members of the European Union deployed mechanisms to manage personal information –and privacy by extension- through the protection of personal data. In that sense, personal data protection is a new form of accountability involving both answerability and enforcement lines as it establishes rules to restraint the processing of "all aspects" regarding our digital lives. Nevertheless, accountability in this scope does not imply deep and external controls over data processors such as surveillance institutions and security forces.

Moreover, whether accountability needs to be related to external controls (in horizontal and vertical directions), data protection rules are jeopardized by a sort of generic narratives about responsibility instead of a real institutionalized supervision. That is, to check the proportionality and justification of the cases that could interfere with data protection rules, the European jurisprudence from the European Court of Human Rights (ECHR) and from the Court of Justice of the European Union (CJEU) is

[2] Charter of Fundamental Rights of the European Union. Official Journal of the European Communities. 12/2000. Available in: http://www.europarl.europa.eu/charter/pdf/text_en.pdf, access date 08/06/2017.

supposed to be a mechanism to supervise and, theoretically, to enforce and turn accountable those organizations who process personal data. The Union also tried to reinforce the roles of data protection Agencies at the national level. Notwithstanding, accountability efforts depended more in critical junctures (leaks, scandals, disproportional security measures) than in defining specific roles and mechanism for the data protection. Therefore, the protection of personal data within judicial scopes in the EU has been very incipient (Sphere Ramiro, 2011).

The mentioned critical junctures were attested in cases such as the "Österreichischer Rundfunk" in 2003. In this case, the CJEU considered that when a national government tracks personal incomes and bank accounts, it interferes with the protection of personal data. However, the CJEU decided that gathering this data could be justified when it is appropriate for the "good" management of public resources (Piñar Mañas, 2003: 61-66). However, the definition of "good" was unclear and unpredictable. Fortunately, since 2012, in cases labeled as "Digital Rights Ireland" the CJEU was persuaded to take legal actions over electronic data retentions provided by the "Criminal Justice Act" (Terrorist Offences) of 2005. In addition, the Court was swayed to decide about personal data transfers to third countries like the United States via private companies like Facebook. The CJEU considered the Act as invalid and claimed for strengthen the European standards in privacy and personal data protection. According to González Pascual (2014), despite the "Digital Rights Ireland" merits, the delay of this sentence can be explained by the "reluctance of the Courts to cooperate" and by their incipient action in this issue (González Pascual, 2014: 953). Another attempt to turn personal data processors more accountable was enhanced when "Google Spain" and the Spanish DPA (AEPD) clashed about the so-called "right to be forgotten". In this case, the Agency established that the manager of a web search engine is also responsible for processing personal data even when the content is owned by third parties (Silva de la Puerta, 2014).

The cases above suggest that accountability was performed through judicial "clashes" rather than by institutionalized efforts or permanent controls and external supervisions. Thus, personal data protection rights usually are defended "a posteriori" and are also reduced to individual contexts, disentangled from several economic and societal players. For those reasons, the legal framework in the European Union was updated by the so-called "General Data Protection Regulation" (approved in 2016 and enforceable in May 2018). In the next section, we will address this reform alongside market practices to manage accountability within personal data scopes.

2. Privacy by Design and market agency

Besides institutional solutions to data protection problems, it is essential to think about the functional dimensions to protect this key information. Thus, an approach beyond the legal rules that cover practices and interactions dealing with personal data are also essential. In this direction, one trend known as "Privacy by Design" (PbD) claims that IT systems designs must take privacy into account since informatics processes to electronic delivering services. For instance, WiFi routers, social networks,

and search engines must provide privacy tools (access controls, encryption, provisions for anonymous use, etc.) embedded to their different functions and purposes.

One extensive definition of PbD derives from the seven acknowledged principles formulated by Ann Cavoukian (2009). These principles could be related to accountability in IT systems as they stipulate: 1. Proactive and preventative measures to counterbalance privacy risks, 2. Privacy protection as default in any IT system or business practice, 3. Privacy embedded at the core functionality of the system delivered, 4. Positive-Sum, not Zero-Sum approach, to avoid false dichotomies, such as privacy vs. security, 5. End-to-End secure lifecycle management of information, 6. Visibility and Transparency, operating according to the stated promises and objectives, subject to independent verification, and 7. User Centric Designs to keep the interests of the individual uppermost by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

In sum, PbD tries to conceal privacy management across IT Systems, accountable business practices, and physical design and networked infrastructure. Despite its comprehensiveness, some people have claimed that PbD ideas to mitigate privacy concerns and achieve data protection compliance remain vague and leave many open questions about their application in engineering systems (Gürses et al, 2011). For Peter Scharr (2010), PbD could be difficult to be translated into practice. For instance, data collectors can articulate the purpose specification to include any data of their liking, eliminating the need to consider data minimization. Even further, companies can limit the reach of solutions that provide by applying anonymization over aggregated personal data, processing activities outside of the scope of data protection rules. The definition of privacy by design is therefore also "susceptible to the interpretation to collect any data as long as it is with a privacy label while shrinking the scope of control from the user" as stated by the seventh PbD principle (Schaar, 2010: 270).

Despite the critiques, market players recognize that privacy must be protected and is a vital component in nowadays e-commerce and business. Beyond the commodification of privacy mentioned above (which still poses a huge value to informational market strategies such as data mining and profiled advertisement), some companies are concerned about "good" practices to manage systems and aggregated data. One example is the ISO.IEC 27000 series of standards on Security Management published by the International Organization for Standardization and the International Electrotechnical Commission. These standards dominate how information security management is done today like in cloud services or telecoms. When an organization obtains a 27001 certification it means that a third party has verified the organization implements on information security and follows some technical requirements which are updated frequently to reflect the new developments and threats in business sectors.

Those and other third parties certifications could be deemed as accountability horizontal strategies with different goals that include trustworthiness and reputation among IT suppliers (important symbols that serve as political coins in this sphere). For instance, a survey from Orange upon its customers mentioned that "fully 78% of consumers think it is hard to trust companies when it comes to using their personal

data" (The Future of Digital Trust Convention, ap. Kearney, 2014). Other companies are immersed in a rhetoric effort to mitigate privacy risks by opposing to the fear and uncertainty that privacy is always traded off against public safety and security.[3] The European Union Agency for Network and Information Security (ENISA) working on information security expertise for the EU and its Member States and The International Chamber of Commerce (ICC), in addition, have defined some similar accountability principles for business organizations in international forums (Figures 1 and 2).

Figure 1: Linking near-term solutions to core challenges

	Transparency	Accountability	Empowerment
Standard data taxonomies	• Drives transparency by creating a common language. • Enables meaningful transparency by filtering what is relevant from what is not. • Facilitates interoperable identity and trust frameworks.	• Provide a baseline for interoperable permissions.	• At the coarse-grained, after level, I can translate technical details into personally relevant themes. • Empowers individuals with context-aware data usage and interoperable data use policies.
Measuring risks and benefits	• Assist data controllers and regulators to set priorities. • Promote global interoperability and leverage existing risk management methodologies.	• Creates a workable measure by which to hold organizations accountable.	• Restructures risk around the concerns and needs of individuals. • Provides institutions with the ability to understand perceived harms through the eyes of individuals.

Source: World Economic Forum (Kearney, 2014)

Figure 2: Linking long-term solutions to core challenges

	Transparency	Accountability	Empowerment
Context-aware personal data management	• Demonstrate that the flow and usage of data (and metadata) is consistent with agreed upon norms and legal requirements. • Meaningful user agreements. With better data accounting, risks can be redistributed.	• Provide the technical means to uphold shared principles in a dynamic, recursive and complex ecosystem. • Strengthen confidence on restitution across jurisdictions.	• Enable individuals to express their unique preferences and controls via metadata. • Individuals can dynamically manage data within a defined context.
Accountable algorithms	• Focus on communicating the intended impact to individuals. • Transparency into the underlying values, principles, decision criteria and outcomes of algorithms.	• Cross-disciplinary "algorithmists" who are collectively responsible for auditing the ethics and anticipated social impact of data driven outcomes.	• Strengthened popular understanding on the economic, sociological and ethical value of the sovereign individual who is both a data producer and consumer.

Source: World Economic Forum (Kearney, 2014)

[3] "Since the Snowden revelations in May 2013 regarding national security surveillance, there has been a scramble for improved encryption services as a measure to protect consumers from surveillance and to win back consumer trust in using ICT services (especially cloud services). However, the use of encryption is not an absolute form of protection – there is an ongoing debate regarding the extent to which the private sector should help law enforcement agencies gain access to encrypted material". United Nations Conference on Trade and Development. 2016. *Data protection regulations and international data flows: Implications for trade and development*, Genève Press: 52.

As observed above, the ICC accountability principles are closely related to Privacy by Design as they try to cover sectors across engineering, business management, and friendly-user environments. Here, transparency enhances accountability that in turn enhances empowerment by near-term and long-term solutions. Those solutions are related to standard taxonomies, risks measurement, context-aware personal data management and accountable algorithms. Adopting those solutions means that data managers need to demonstrate "that the flow and usage of data are consistent with agreed upon norms and legal requirements" (Figure 1). In addition, "strengthen confidence" and "empower individuals" over personal data are at the core of the systems and its functionalities. Moreover, risk analysis assessment is as essential as auditable algorithms. The latter must be done to "anticipate the ethical and social impact of data usage" (Figure 2). At first glance, those solutions could be deemed as trivial ones. But in fact, they have introduced a new paradigm for business practices which cannot be neglected to analyze politics delivered by market players, especially when they foster reforms on personal data protection.

The close relationship between the market agency and state legislators could be attested in the mentioned "General Data Protection Regulation" (GPDR). Approved in 2016, the GPDR is valid if the data controller or company (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU. According to the European Commission, "information relating to an individual such as a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address"[4] is covered by this regulation. The GDPR affects especially market and societal practices and unfortunately its terms do not apply to the processing of personal data for national security purposes or law enforcement inside a Member State.

Due to that scope, the GDPR demands that data controllers should implement measures in accordance with the principles of data protection by design and data protection by default. It explicitly mentions the term "Privacy by Design and by Default" (Article 25) requiring data protection procedures since the design of business systems to the products and services. Moreover, Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is mandatory for high risks. Data Protection Officers (Articles 37–39) are to ensure compliance within organizations. In addition, the Article 47 stipulates DPA independence as each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation. These points are closely linked to those ones exposed in the figures above, such as risk assessment and corporate accountability. Digital management in market

[4] 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. Available in: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, access in 18/09/2017.

[4] Peter Schaar. Privacy by design. Identity in the Information Society, 3:267{274, 2010.

spheres and data protection regulations have never been so related and interdependent. The GDPR bets for a reform that facilitates digital market practices and information exchanges. Besides, it privileges accountability functionality dimensions over institutional lines as a way to overcome the thresholds of the Directive 95/46/EC, mentioned in part 1. For instance, private organizations need to incorporate internal oversight accountability principles (such as horizontal audits and risk assessment) and personal data files must be processed according to the scope and range of each company. There is no obligation to maintain data copies in a DPA. However, data breaches and security deficits must be communicated immediately to the DPA (Article 33).

Despite the transference of prerogatives to implement "good" practices in each company, the GDPR brings new challenges up as it is enforceable since May 2018. Firstly, the GDPR will require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy before the regulation entered into force (especially non-European companies handling EU personal data). Secondly, the Article 83 stipulates general conditions for imposing administrative fines according to the nature, gravity, the number of data subjects affected and the level of damage suffered.[5] Such fines are clear points that support enforcement accountability mechanisms (p. 4), avoiding a toothless regulation, and binding companies to adopt privacy by default measures. Since the DPA cannot lead with the bulky information collected from the data processors, it is reasonable that institutional roles must be complemented with a regulation that enhances capillarity to penetrate organizational functionalities in order to accomplish accountability principles.

In sum, the gathering of personal information entails a duty of care and protection beyond legal regulations. Data protection must be a duty for all players dealing with digital flows. Nevertheless, we must be skeptical as Privacy by Design and other "good" practices could become fuzzy and elastic enough to be applied to any informational system. "Given such a fate, […] privacy by design would risk being damaging to all involved: if the principles are applied loosely, it would lead to a false sense of privacy and trust, until the term looses its reputation enough to become meaningless" (Schaar, 2010).

Furthermore, if the purpose of any system is to do intrusive surveillance of populations, then privacy by design labels could be misleading. The creation and discarding of the German ELENA Data System on Social Security and Labor (Elektronische Entgeltnachweis), which was developed according to the principles of PbD, attested the complexities to combine engineering design and data usage for third purposes. The ELENA Data System represented a clear example with good intentions that did not overcome open problems in the intersection between technical formulation and policy making. When state rooted regulations meet market preferences, some

[5] Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Official Journal of the European Union. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

difficulties might emerge within this relationship or even beyond it. Thus, the next part analyses the role of civil agency in the face of the previous limitations and as a sphere that can fill accountability demands.

3. Civil agency interactions

As government regulations encountered the market agency to manage accountability in digital flows, a major concern is whether this principle will follow the path of e-democracy and online deliberation, which still struggle to be seen more than tokenistic exercises to engage with the public. A real connection with citizens through virtual networks still represents a challenge for vertical and centralized governments "used to dealing with restricted groups that speak with one voice in the language of advocacy" (Coleman and Blumler, 2009). In the other hand, the civil agency can be defined as being a multifaceted and pluralistic interaction delivered by social players that are either permeated or situated outside the traditional locus of government and market.

> Online civic and political networks are less likely to advocate a single ideological position (although they sometimes do) than reflect a set of values, experiences and reflexive disclosures of identity […]. Governments prefer to deal with settled public interests expressed as aggregate demands than informal collectivities working towards a common identity through mutual disclosure. Those who are active within civic and political networks do not necessarily know what they demand: they are searching for articulations of their interest through a process of ongoing production of and exposure to new knowledge.[6]

The array of civic interactions and interests as attested by the quotation inhibit an ultimate conceptualization of civil agency. Yet, there are alternative models for accountability besides that of the democratic state which may have closer application to governance networks in some respects. On the one hand, within the institutionalized dimension, this approach can be demonstrated in the model which The Internet Corporation for Assigned Names and Numbers (ICANN) has employed. Though somewhat jeopardized by stronger voices such as its implicit US allegiance, the ICANN adopted a participatory democratic line of open public comment before policymaking and it has institutionalized mechanisms of review (Malcolm, 2008). On the other hand, public preferences could be detached from institutional boundaries. A strong civil society lying outside the power of the state (or official governance networks) is another important influence upon a network's public accountability, and so too, once again, is an independent mechanism of answerability that may as well spark enforcement.

In that sense, hacking is one example of amorphous but important stream of cyberpolitics. Despite their several categories (novices, cyber-punks, ethical hackers, hacktivists, crackers, insiders, criminals and government agents), it has the potential to

[6] Coleman & Blumler, 2009: 135

either undermine or engage with accountability principles. In the last case, Tim Jordan (2007) differentiates two groups that engage with radical democracy in contrasting fashion: Mass action hacktivism and Digitally correct hacktivism. The first group focuses on political legitimacy based on masses of simulated bodies by producing technologies with impaired or less than optimal functions. They are most closely related to communities that constitute alter-globalization or global justice movements. The second group works from a political legitimacy based on the human right to freely and securely access information. This group can use sophisticated interventions in the technological fabric of the Internet and is most connected to open source and human rights activist communities. "Mass action hacktivism's puts radical democracy at the center of their aspirations, whereas digitally correct hacktivism's deep concern for free, secure access to all information focuses them towards the infrastructure of information" (Jordan, 2007: 75).

We can argue that the tactics to facilitate free and secure access to the largest information network for humanity could be deemed as enhancers of accountability mechanisms. Despite being distant from Schedler or O`Donnell accountability principles, it is clear the potential of those actions to ensure that information management does not collapse into a de-facto struggle for domination in the hands of powerful players. Digital correct hacktivists supporting Open Codes to diminish barriers that limit the access to information and knowledge are actually behind common applications and software on the web. Open Codes are used either to boost commercial applications or to develop efficient Privacy Enabling Technologies (PETs)[7]. Moreover, commercial software does not allow permanent code audits as those made by public forums and users. These vulnerabilities, therefore, are exploited by security agencies to attack systems or implement backdoors.[8] At the same time, Denial of Service attacks and encryption technologies can also be used to mitigate the misuse of personal data or to counterbalance surveillance abuses. The most famous digital leaks on national security issues in the West during the last years (such as the Snowden and Manning revelations and Wikileaks cables) resulted from a level of commitment against the indiscriminate use of information to profile, categorize, discriminate, or stigmatize people based on regular behavior or specific ideas. It cannot be possible to think in filling the gaps or to enable direct accountability efforts without the struggles between those who maintain or facilitate critical information to certain audiences. A comprehension of the social, political and economical conceptions of accountability must be oxygenated with informal attempts to expand digital public spheres beyond the institutional and functional limitations as attested in the previous sections.

All the same, as the global economy shifts further into a connected information space, the relevance of data protection and the need for controlling privacy will further

[7] Boucher, 2011.

[8] One example of the technical vulnerabilities exploited by security agencies, such as the US CIA, was released in a series of documents acknowledged as "Vault 7". The last cyber attacks that launched "ransomware" over several computer infrastructures during April, 2017 also exploited fail updating shields in private software. The Guardian. What is WannaCry and why is it attacking global computers? 04/12/2017. Available in: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20, access date 12/07/2017.

increase. The 2016 United Nations (UN) Conference on Trade and Developments recognized the importance of data protection regulations and international data flows for commercial and civil purposes.[9] The UN encouraged actual collaboration amongst multi-stakeholders and non-institutional partners to expand the communicative scope of interaction on the web. Besides, there was a claim to balance surveillance and data protection. However, being open and accessible cannot automatically guarantee horizontal and universal participation. Elena Pavan (2012) exploration of online networks, for instance, demonstrated a high degree of fragmentation in communication patterns. For Pavan, active exchanges of opinions and virtual forums play merely an informative role in the majority of occurrences. "Compared to others, perhaps more urgent, international issues like global justice and peace, environmental concerns, etc., Internet Governance demands greater communicative and mobilization capacity to raise more attention among audiences" (Pavan, 2012: 112). For those reasons, some gaps still remain untouched when it comes to foster deep democratic actions regarding digital information, especially in terms of accountability.

To fill those gaps, some scholars have suggested counterbalancing hegemonic practices on the web with a coordination of interests via open communication. Joss Hands (2007) and deliberative supporters value "Not agonism, but agreement/disagreement underpinned by reciprocity […]. Not an articulation of social movements, but free association and affiliation […]. Non-proprietary interaction and guaranteed universal education and access to CMCs". Meanwhile, feminist and poststructuralist critics argue that deliberative approaches ignore communicative 'distortions' (including exclusions) resulting from coercion, instrumental-strategic action, social inequalities, and technical limitations (such as in the technologies used). For instance, Lincoln Dahlberg (2007) emphasizes the agonistic relation to constructing interactions on the web. To be aware of the exclusionary aspects of the web, as technology is never detached from offline power asymmetries, must prevail over different criteria to replenish social activism and foster radical strategies of contestation.

Despite the differences in the social agency interactions, it does not imply that people assume a deterministic vision of counter-publics, rather, it means a co-edification effort embedded to mutable strategies for waking provisional realities up in the face of altering and parallel political forces. Therefore, accountability, and other democratic principles, are not defined a priori as they serve as "auxiliary precautions against the potential for the regression of democracy into hierarchical forms such as bureaucracy or oligarchy, which in turn may offer a mask for inefficiency and corruption" (Warren, ap. Malcolm: 2008: 260).

Though the quantifiable impact of the internet on the contemporary civil agency is still debatable, an increasing occurrence of web-based strategies, networks structures, and democratic organizational communications represent an important step. This step

[9] "The rules surrounding data protection and cross-border flows of data affect individuals, businesses and governments alike, making it essential to find approaches that address the concerns of all stakeholders in a balanced manner". UN Conference on Trade and Developments: Implications for trade and development, 2016.

suggests that internet technology remains a porous place for democratic, even radical, potentials. However, digital networks are not miraculous self-generating spaces.

Conclusion

When it comes to the democratic potential enhanced by digital networks, it is necessary to move forward from debates who celebrate new democratic forms unleashed by internet technologies and those who lament the lost promise of the initial Internet. In terms of deeper democratic practices, five principles were mentioned. One of them is related to accountability, either by answerability or enforcement principles. These principles were analyzed in digital flows, specifically in terms of personal data management in Europe. In that sense, we considered three complementary spheres: state-rooted regulations, market agency, and societal agency.

In the first sphere, data protection has been enshrined as a fundamental right in the European Union. The European jurisprudence based on Directive 95/46/EC was initially concerned in strengthen institutional dimensions, such as in defining the roles and scopes of Data Protection Authorities. Complains about its reactive and sporadic resolutions do handle data breaches and misuses are hoped to be mitigated with the new General Data Protection Reform (GDPR). Enforceable since 2018, the GDPR is an extensive legislation that could be deemed as a market-oriented reform attempting to introduce principles from Privacy by Design, Risk Assessment, and User-centered management. Those topics were deemed as ideal accountability approaches within privacy organizations and business environments as attested in the second sphere. The new European legal framework, in that sense, privileges functionality dimensions for accountability beyond institutional boundaries.

Nevertheless, criticism remains as Privacy by Design does not necessarily address methodological aspects of system engineering, such as complete data lifecycle and anonymous content. Moreover, it has been pointed out that the new regulation, and a market self-oversight, could be similar to voluntary compliance in industries impacting the environment. Despite the scheme of fines and prosecution, the efficiency to implement accountability principles may differ in every company. Some critics have pointed out that certain business models are built around customer surveillance and data manipulation and therefore voluntary compliance is unlikely (Rubinstein and Good, 2013).

In additions, it was essential to analyze accountability practices beyond managerial rules. In this case, the civil agency was deemed as a third sphere that can either undermine or strength the so-called commodification of privacy adopted by some informational data processors. Whereas the first two spheres (state-rooted rules and market agency) may conceive the public as policy or product consumers rather than politically active agents, distant positions have been pointed to accountability problems. Citizens addressed as consumers or conceived as pure demands, and governments seen as providers, endorse a curtailed relationship and a self-restrained notion of democracy,

where individuals are passive subjects and institutions are mere suppliers of correct norms and good practices to deliver services.

By stirring this notion up, the civil agency has shown that it has not lost its potential to fill the gaps to spark or accomplish accountability principles. Either by supporting Open Codes or by restraining surveillance abuses, Mass action hacktivism and Digitally correct hacktivism were just some examples of civil awareness to strengthen the freedom of information and to democratize the use of digital flows. Despite the differences in the social agency interactions, these represent strategies of political co-edification in the face of hegemonic political actions. Therefore, accountability here serves as an auxiliary (not substitutive) tool against cooptation from activist strategies as well as dire manipulation of digital information. The quantifiable impact of the Internet on contemporary activism and politics is still debatable and escapes our objective. However, it is essential to reconsider the nuances between naive and fatalistic interpretations about the interactions of distinct political players and their strategies to strengthen accountability by formal or informal paths. It is meaningless to develop essentialist approaches seeking the "actual" or ultimate characteristics about the Internet players and their politics. At the same time, deterministic approaches that abolish the essential roles and the vital action of the civil agency (and its array of movements) are equally worthless to analyze the mutable social fabric where we live and communicate.

References

Andrejevic, M. (2011). *Surveillance and alienation in the online economy*. Surveillance & Society, 8(3), 278.

Sphere Ramiro, M. (2011). *Los cambios previstos en la Directiva 95/46/CE de protección de datos personales*, Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 50, abril.

Beer, D., & Burrows, R. (2010). *Consumption, prosumption and participatory web cultures*: *An introduction*. AP Press.

Boucher, D., & Flowerday, S. (2011). *Privacy: In pursuit of Information security awareness*. In ISSA.

Blaug, R. (2002). *Engineering Democracy*. Political Studies, 50(1): 102–16.

Byung-Chul, H. (2012). *La Sociedad de la Transparencia*, Madrid: Herder.

Castells, M. (2011). *The rise of the network society: The information age: Economy, society, and culture* (Vol. 1). John Wiley & Sons.

Cavoukian, A. (2009). *Privacy by design. Take the challenge*. Information and privacy commissioner of Ontario, Canada.

Coleman, S., & Blumler, J. G. (2009). *The Internet and democratic citizenship: Theory, practice and policy*. Cambridge University Press.

Collier, R. B., & Collier, D. (2002). *Shaping the political sphere*. Notre Dame, University of Notre Dame Press.

Dahlberg, L. (2007). *The Internet and discursive exclusion: From deliberative to agonistic public sphere theory.* Radical democracy and the internet: Interrogating theory and practice, 128-147.

Deleuze, G. (1995). *Postscript on control societies*. Negotiations: 1972–1990, pp. 177-82.

European Information Society Forum Report, 1999. *Connecting to the information society: a European perspective.* Stephanidis C., & Emiliani, P. L. Technology and disability, 10(1), 21-44.

Gray, R., Owen, D., and Adams, C. (1996). *Accounting & Accountability: Changes and Challenges in Corporate Social and Environmental Reporting*. London: Prentice Hall.

González Pascual, M.I. (2014). *El TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland.* Revista de Derecho Comunitario Europeo, 49, pp. 943-971.

Gürses, S., Troncoso, C., & Diaz, C. (2011). *Engineering privacy by design*. K.U. Leuven/IBBT.

Haggerty, K. D. and Ericsson, R. V. (2000). *The surveillant assemblage*. British Journal of Sociology Vol. No. 51 Issue No. 4 (December 2000) pp. 605–622.

Haggerty, K. D. and Samatas, M. (2010). *Surveillance and democracy: an unsettled relationship*, in Haggerty, Kevin D. and Minas Samatas (eds.), Surveillance and democracy, London: Routledge.

Hands, J. (2007). *Between agonistic and deliberative politics: towards a radical e-democracy*. Radical Democracy and the Internet: Interrogating Theory and Practice, New York: Palgrave Macmillan, 89-107.

Hiltz, S. R. Turoff. M.(1987). *The network nation: Human communication via computer*.

Jordan, T. (2007). *Online direct action: Hacktivism and radical democracy*. In Radical democracy and the internet (pp. 73-88). Palgrave Macmillan UK.

Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes*. Washington, DC: Carnegie Endowment for International Peace.

Kearney, A. T. (2014). *Rethinking Personal Data: A New Lens for Strengthening Trust*. In World Economic Forum. Retrieved November (Vol. 1).

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*. Terminus Press.

Margolis, M. and Resnick, D. (2000) *Politics as Usual: The Cyberspace 'Revolution'*, Thousand Oaks, CA: Sage.

Nevin, D. J., & Jenkins, M. (2014). *Information, Knowledge, and the Pursuit of Privacy*. Am. J. Trial Advoc., 38, 485.

Noam, E. (2002). *Why the Internet Is Bad for Democracy*, Communications of the ACM, 48(10): 57–8.

Pavan, E. (2012). *Frames and Connections in the Governance of Global Communications: A Network Study of the Internet Governance Forum*, UK: Lexington Books.

PGA. Promoting Global Accountability Project (2008). *The Experiences of the Global Accountability*, Project Author(s): Robert Lloyd Source: Global Governance, Vol. 14, No. 3 (July–September 2008), pp. 273-281

Piñar Mañas, J. L. (2003). *El derecho a la protección de Datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas*, Cuadernos de Derecho Público, n. 19-20, Mayo-Diciembre, 2003, pp. 61-66.

Raab, C. (2013). *Increasing Resilience in Surveillance Societies*, The University of Edinburgh: IRISS project.

Rubinstein, I. S., & Good, N. (2013). *Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents*. Berkeley Tech. LJ, 28, 1333.

Schaar, P. (2010). *Privacy by design.* Identity in the Information Society, 3(2), 267-274.

Schedler, A. (1999). *The self-restraining state: power and accountability in new democracies*. Lynne Rienner Publishers.

Silva de la Puerta, M. (2014). *El 'derecho al olvido' como aportación española y el papel de la Abogacía del Estado*, Actualidad Jurídica Uría Menéndez, 38, pp. 7 - ss.

Thompson, J. B. (2005). *The New Visibility*, Theory, Culture & Society, 22(6): 31–52.

United Nations (2016). *Conference on Trade and Development. Data protection regulations and international data flows: Implications for trade and development*, Genève Press.

Warren, M. E. (2006). *Controlling corruption through democratic empowerment: Market-style accountability reconsidered*. In: Annual Meeting of the American Political Science Association Philadelphia, August 2006.