From Governmental Vigilance to Diffuse Control: Surveillance and Accountability since the Spanish Transition

Jaseff Raziel Yauri Miranda

https://doi.org/10.22151/politikon.32.2

Jaseff Raziel Yauri Miranda is Ph.D. student in "Society, Politics and Culture" at the University of the Basque Country (UPV-EHU). Master degree in "Governance and Political Studies" also at UPV-EHU and Degree in "History" with complements in Political Science at the Federal University of Minas Gerais (UFMG) in Brazil. He was member of the "Center for Strategic Studies and Intelligence" (CEEIG-UFMG) and currently is the Chair of the "International Law and Governance" Student Research Committee in the "International Association for Political Science Students" (IAPSS).

Abstract

Considering the inertia of past institutions and practices, this paper questions how the accountability of surveillance has been affected in terms of its quality and mechanisms. To verify this, the first part depicts the background related to intelligence institutions since the Spanish democratic transition in the late 70s. The second part is focused on digital personal data flows in a de-concentrated surveillance assemblage since the 90s. On each part, the accountability mechanisms are analyzed through a historical and political methodology based on the theory of legacy constraints. Structured bibliography related to checks and balances and the analysis of legal measures regarding the protection of privacy are the sources for this study. The conclusion alludes to a posteriori mechanisms of answerability and to uncoordinated efforts of accountability since the first period. It also stresses the importance of answerability promoted by the citizenship to complement and reinforce enforcement dimensions which are affected by the secrecy of surveillance.

Keywords

surveillance, accountability, intelligence services, personal data, democratization process

Introduction

The historical experience of present-day democracies has a significant influence on how citizens react to and cope with surveillance. Throughout the recent past, several repressive regimes have built surveillance networks and institutions with and against their citizens. Haggerty and Samatas (2010) claim that surveillance, as a starting point, seems to be antagonistic to democracy, and ultimately lead to totalitarianism. However, surveillance could be a legitimate element of democratic systems as well. And one of the fundamental differences between dictatorial and democratic systems with regard to surveillance lies in its accountability. Even when state surveillance cannot be overseen and controlled by the citizens, at least in an institutionalized form, the so-called democracies must have an acceptable ground of institutions and mechanisms established for this purpose (although in practice such systems cannot be easily recognized nor controlled).

Thus, this paper aims to identify and analyze the relation between surveillance practices and accountability, focusing on the Spanish scenario since its last democratization process. Furthermore, since the end of the Franco regime, the essential objects for the analysis are the sensitive information gathered from individuals by surveillance institutions, the accountability mechanisms of these institutions, and the limits of accountability itself. In doing so, it is expected to contribute to two fronts: the first is related to political science, and within it, to accountability studies and security politics. The second one is related to historical studies, especially after political violence periods and state authoritarian experiences. We consider that past societies matter and are also complex refusing the common explanation that present time is a priori more complex than previous periods. Therefore, we adopt a historic approach for analyzing the past since it can help us to rewrite and understand today surveillance practices. Nevertheless, we go further as past experiences are added with new keys, paradoxes, and challenges, especially in our informational society.

Theoretical framework and conceptualization

Considering the surveillance practices, the literature underscores a diffuse and decentralized surveillance era where "all aspects of life" seem to be spotted by technological and liquid "assemblages" (Haggerty and Ericson, 2000). Nonetheless, the arrays and interpretations differ on the validity of the classic "Panopticism" as this concept served to understand the origins of the western surveillance. The panoptic concept, originally formulated by Jeremy Bentham and then readapted by Michel Foucault (2014) in "Surveiller et punir", is a sort of imprisonment metaphor used to describe a situation where the overseen are expected to internalize a continuous state of vigilance and self-discipline. Foucault adopted this concept to identify several discipline "areas" where individuals are shaped and are overseen by "watchers". And because of the several areas, gazes and bodies where vigilance can be deployed, Foucault

understood multiple surveillance worlds which are opposed to an "Orwellian Panoptic or to a huge and simple Leviathan" (Caluya, 2010: 623).

Nevertheless, the panoptic metaphor still frightens our mind. Firstly, some authors such as Norris & Armstrong (1999) and McCahill (2001) argue that the current surveillance practices are opposed to the unidirectional and centralized Panopticon. The validity of the Panopticism concept is retained for them but as Majid Yar (2003: 257) underscores, "its applicability is contingent upon the extent to which circumstances reproduce the conditions in which it finds its effectivity (…)". Moreover, "its deployment is analytically justified and subject to empirical limits". As a second interpretation, scholars such as Deleuze (1995), Bauman (1998), Diken and Lausten (2002) argue that the contemporary societies experience the dissolution of institutional boundaries -and with it the dissolution of sites in which panoptic technology previously found its disciplinary function. In that sense, we face a "Post-panopticism" concept. In addition, it is possible to formulate a separation between two historical stages, or between the "disciplinary societies" and the Deleuzian "control societies". Finally, a third interpretation try to conceal both diagnosis by combining the conviction that the Panoptic concept still can perform a valuable understanding, so long as it is "either refined and reformed appropriately in light of changing circumstances, or its status as ideal type rather than empirical generalization is clarified and recalled" (Yar, Majid, 2003: 258).

In light of the above, the theoretical interpretations about surveillance express a phenomenon opposed to a centralized and fixed idea. Since this phenomenon has become decentralized and fragmented, it is possible to adopt a flexible and "long duration" definition for the last decades: surveillance consists in the act of seeing without being seen and in social control –the act of shaping social behavior by watching and controlling (Mathiesen, 1997). We adopt this starting definition paying attention to the fact that surveillance can assume a plethora of institutional forms and social contexts. For that reason, we apply that definition –the act of seeing without being seen, and the act of shaping social behavior by control- to a narrower social aspect: the act of gathering private citizens' information by institutions that are supposed to govern in a democratic context.

As the legacy of previous experiences is a key to understand surveillance practices, "post-dictatorial" scenarios and democratic transitions allow us to apprehend the de-concentration, decentralization and emergence of new surveillance arenas, as argued by most of the scholars. In addition, this article adopts the legacy constraints framework to analyze the accountability efforts to control vigilance. Legacy constraints suggest a theoretical framework stemmed from studies such as critical junctures, path dependence and new institutionalism. The legacy constraints refer to historical discontinuities and small revolutionary changes that are influenced but still reproduce past institutions and practices. For instance, they are related to critical junctures, a period of significant changes occurring in different ways and places

which is hypothesized to produce distinct outcomes if not considered as an explanation (Collier and Collier, 2002). At the same time, this concept is intertwined with other logics, such as the path-dependence theory (David, 2007) which asserts that social outcomes are difficult to modify due to previous policies. In short, legacy constraints emphasize the impact and dependency on previous conditions and practices, either by historical events or political decisions.

Moreover, legacy constraints do not imply that previous politics and values are intrinsically worst than new ones. It implies a political dependency which affects and is reproduced from the past until an unpredictable ending. As the ending time is unknown, the paths opened by the origins are essential. Similarly to the historical institutionalism studies (Pierson and Skocpol, 2002; Immergut 2006; Steimo, 2008), the legacy framework express an institutional inertia that marks the trajectory and development of political arenas. In that sense, previous organizations and legal configurations affect certain issues, especially in the case of security. Yet, no single model of change or the impact of past events can do justice to the multiple levels of causality at work in historical explanations. Instead, general units of analysis (such as institutions, laws and practices) can be used to pose questions and find answers regarding a particular case or phenomenon (Immergut, 2006). Thus, the institutions of surveillance, as well as their practices, represent a background worthy of consideration in order to analyze influences, reactions, cooperation and conflicts related to democratic efforts such as accountability.

The definition of accountability comes from the theory formulated by Andreas Schedler (1999). According to Schedler, accountability is a bi-dimensional concept which consists in answerability and enforcement. Answerability means the act, capacity and prompt response of those actors that are held accountable. It makes the accountable and accounting actors engage in a public debate or in the light of the public interest (Schedler, 1999:15). Enforcement is a call for punishment to 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 are mechanisms of accountability as well (Schedler, 1999: 17). At the same time, Guillermo O'Donnell (apud. Schedler, 1999) makes 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 or policy makers in a context of a decision.

This article analyzes surveillance institutions and practices in the light of the two dimensions expressed by Schedler and by using the horizontal and vertical relations of O'Donnell. These concepts are basic for further definitions. For instance, as stated by Charles Raab (2013: 46), "surveillance institutions ought to

be accountable to the governed, to those whose information they handle and to others who may be affected by surveillance 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. In post-authoritarian and democratic scenarios, transparency has to do with reviewing and understanding the surveillance systems that surround the citizens. Thus, accountability, from a functional perspective, virtually works the "same way as surveillance does, but the other way around: as surveillance provides a method of control over citizens for surveillers, so does transparency for citizens over their surveillers" (Lyon, David, 2007: 156). To summarize, accountability in surveillance could be worked within the concepts of answerability and as a tool to oversight the use of individuals' information with a satisfactory degree of regulated secrecy and inside legal and democratic principles.

Methodology

Considering surveillance past institutions and practices in the Spanish democratization process which continues to the present day, as hypothesis it is questioned how an accountability project has been affected in terms of its quality and its mechanisms (answerability and enforcement). To verify this, it is necessary to depict the political background related to surveillance institutions and practices. Once these surveillance marks are reconstructed, it will be possible to analyze how the accountability mechanisms were affected in the face of surveillance. Finally, if the vigilance logics still heavily defy those mechanisms, it is necessary to question how the accountability mechanisms can be reconfigured in order to improve it.

To proceed with this, the article has been divided in two periods. The first one begins after the Spanish democratic transition in the late 1970s, which was marked by a governmental and quasi-centralized surveillance system in the hands of intelligence institutions. The second period is initiated after the Cold War and is characterized by the "crisis" of national state forms as central political players and by technological shifts since the 1990s. As institutional boundaries became blurred and were replaced by digital logics, the object of the paper is shifted to personal data. In the latter period, it is possible to include the development of a European level, which among several institutions, has fostered actions to turn surveillance practices more accountable, at least on a legal base.

In the first period, the collection of information can be associated with the end of the Franco regime and its marks on the new security agencies. Consequently, it is of interest to question how accountability and transparency were interpreted in those times in a new democracy. What were the internal and external controls? To answer those questions and avoid anachronisms, the surveillance practices were associated with the nature of the democratization process, the "spirit" of the time and its rhythm, which in Spain

was remarkable known as an arranged process. In this part, the sources were historical and political bibliography translated from Spanish in order to do a qualitative analysis of the intelligence institutions of the period and its democratic control.

In the second period, the gathering of personal information could be linked to shifts in market practices, non-government actors and supra-national institutions since the 1990s. We understand that states still play a key role in the surveillance world but, at the same time, other organizations and "watchers" dispute personal and private information. How is surveillance of personal data shaped and worked in diffuse and multilevel assemblages? What are the types of accountability? In order to answer those questions, judicial sentences, laws and decrees regarding protection of personal data were the main sources as these represent a front to restrain indiscriminate surveillance practices (such as the ones regulating the Spanish Agency of Data Protection and the sentences of the Court of Justice of the European Union, CJEU). Finally, bibliographic analyses related to these productions both at the Spanish and European levels have complemented this part.

A quasi-centralized node of information

After the death of Francisco Franco in 1975, Spain initiated the so-called democratic transition by the popular elections in 1977 and the promulgation of the Constitution in 1978. The transition initiated new endeavors to bring the surveillance institutions that served Franco's regime toward the lights of a new era. By then, the greatest institution in this field was the "Superior Center of Information and Defense" (CESID). This organization was created on July 1977 and replaced the "Third Information Section of the Military Staff" and the "Central Documentation Service" (SECED).

Back in the past, the SECED replaced the "Counter-Subversive Organization" (OCN), which was created in the last years of the Franco's regime to prevent and contain the May 1968 social movement. Researchers such as Francisco Zorzo Ferrer (2005) suggest that at those times neither the police nor military forces were able to control student strikes. Therefore, Colonel José Ignacio San Martín "initiated undercover operations at universities to forestall radicalizations" (Zorzo Ferrer, 2005: 85). These operations aimed scholars, unions and religious groups. Later on, their achievements were institutionalized in the SECED form. In that sense, Díaz Fernández (2005) affirms that good relations between San Martín and his superiors, including the Presidents of the government, promoted the SECED into a new level as they offered new infrastructures, staff and information. In a few years, each Ministry or Executive Office was settled by one or more SECED members whose functions were to supply the "Center" with fresh and valuable information. These methods allowed the new governments to spy on internal opponents and to monitor radicalization of military groups because some of them wanted to abolish the arrangements of the transition (Díaz Fernández, 2005: 207).

Scholars like Peñaranda Algar (2005) suggest that the relative success of the SECED was a result of the political identification among bureaucrats and high policy makers. However, after the failure to prevent a military "coup d'état" in 1981, which included the participation of SECED ex-leaders, including San Martín, the "Central" fall into discredit and was transformed into the "Superior Center of Information and Defense" (CESID). Due to this transformation, the CESID experienced a relatively long period of stability which in terms of organizational procedures consisted in a phase of centralization, followed by a delegation process that concluded with a period of "coordination dilemmas within the information/intelligence community" (Díaz Fernández, 2006: 29). We can deduce those dilemmas as a proof of the decentralization and "blurriness" of borderlines in the surveillance world, which were reported in the theoretical framework. In that sense, the Spanish intelligence community was also affected by scandals that emerged in 1995 due to illegal interception of communications, that is, due to a lack of control and accountability. These episodes culminated with a new reformulation as the CESID was transformed into the "National Center of Intelligence" (CNI), in 2002.

More details about the accountability mechanisms will be exposed further on. Yet, it is acknowledged that the procedures that paved the road to collect personal and private information by CESID (and by its predecessors) were plenty. As we pointed above, in many cases this kind of information was facilitated by officials deployed in the Ministers or Executive Offices. For instance, since the OCN times, a communication channel was established by the "Dirección General de Seguridad" (General Office of Security) and the "Dirección General de Política Interior" (General Office for the Interior Policy), with the latter offering hundreds of personal records collected by police agents in many cities. It is worthy to mention that each of the "Secciones del Estado Mayor" (Military Ministries Offices) and the "Comisaría General de la Polícia" (General Police Department) also owned agencies to collect sensitive information, but their structures were "smaller" than the SECED and the CESID (Peñaranda Algar, 2005: 100-102).

Furthermore, the SECED used a file's system called "Janus" to store hundreds of records from people who played (or might potentially play) a prominent role in the democratic transition -in favor or against it. By including their two "faces", the public and the private, the system recalled the Greek myth of a double-faced figure as it created "complete profiles about politicians or suspects, including their properties and incomes" (Díaz Fernandez, 2005: 207). Besides that, the system relied on two major divisions that continued for decades: the Information and Operations divisions of SECED and CESID. as mentioned above, the divisions were mainly deployed in educational-intellectual, labor and religious arenas. They were also instructed by the "Psychological Actions Office, the Department of Special Affairs and the General Secretariat, which provided valuable information even from open sources" (Zorzo Ferrer, 2005: 90).

Alongside the "Janus" System, the SECID used to collect information by other channels. For example, as it depended on the Defense Office, the "Center" was supported in tasks such as "cryptanalysis and decryption through manual and electronic procedures" (Ruiz Miguel, 2005: 138). To afford those activities, surveillance organizations like SECID obtained special funds from the national budget via the "General State Budget Law". Whereas this Law established a percentage of the resources to each national agency, complementary resources came from the "Reserved Funds", a sort of monetary fund to cover Defense and National Security expenditures. When comparing to other national budgets, the Reserved Fund was classified as official secret regarding its details and goals. Even nowadays, "Any information related to the appropriations or usage of the Funds has a secret classification" (Law 11/1995, May 11th) and can be declassified only by the council who established its closure and through a parliamentary petition.

By those procedures and financial support, the "Center" extended its capacity to different targets and organizations. This expansion enabled different results that not always have been positive for the SECID. Yet, the range of relations or network was so broad that it covered organizations such as:

> The Ministry of the Interior, the Ministry of Information and Tourism, Ministry of Education and Science, Trade Union Organization, Ministry of Labour, General Secretariat, the National Youth Delegation and the National Delegation of Women's Section. The exception was the Ministry of Foreign Affairs, presumably because the information coming from abroad belonged to the High Command Military scopes. (Peñaranda Algar, 2005: 100).

The intelligence node or network, as stated by Antonio Díaz Fernández (2005), was clearly a key player in the Spanish transition. There is no doubt that the biggest organization which implemented surveillance measures to collect personal information was the CESID. Previously, it monitored political radicalizations against the "top-down"' arranged transition. Later on, the CESID was a tool to monitoring terrorist groups such as the Basque ETA – especially during the "dirty war" in the 80s. As the democratization process was being deployed, it was necessary to restrict the CESID practices of espionage on politicians and citizens. At least it was essential to build more controls over the surveillance practices. In that sense, a phrase suggested by an ex-leader of the service, Gutierrez Mellado, is very elusive: "the CESID could not simply wish to bring the militaries to a democratic culture. However, it was easier and convenient for them to obey the orders coming from the new political government" (Díaz Fernández, 2005: 213).

When the service tried to adapt itself to a new democratic regime, it was a result of the political pressure since the 1980s, as Spain aimed to transform its secret services in a broader sense. That is, it was necessary to adopt new informational logics and abandon old doctrines in order to show consonance with the roles

assumed in the North Atlantic Treaty Organization (NATO) and with the European Union (Díaz Rodríguez, 2005: 27; Aba Catoria, 2002: 144). But the renovation of the secret services has been, and not only in Spain, a battlefield with many fronts and situations. The mechanisms that addressed the CESID practices in order to turn it more accountable are analyzed below.

Accountability on the move

The "Superior Center of Information and Defense" (CESID) was under control of the Ministry of Defense and it was also configured as an organ of the State responsible for the management and coordination of the National Defense policy.[14] At the same time, the sources and methods of the institution were classified as official secrets. Therefore, as a starting point, this opacity was a considerable challenge for any kind of external accountability. Ultimately, during the 80s, it cannot be said that the CESID activities were object of any type of control aside from the hierarchical one handled by heads-chiefs and commanders (Aba Catoria, 2002).

Despite the lack of controls, especially in the first democratic governments, some authors such as Antonio Díaz Fernández claim that the activity of SECED was focused on gathering information and developing psychological operations rather than interfere directly with target groups. However, if the "Center" usually had not participated in direct actions, it has provided information which "was useful to other agencies that executed violent actions" (Díaz Fernández, 2005: 209). Moreover, it must be underscored that information collected by surveillance activities was only regulated for cases investigated by police and justice officials. Regarding espionage to gather citizens' information by "unconventional" ways, these practices were only mentioned in internal manuals as "special techniques in intelligence operations" to perform actions by "the requiring procedures or necessary means" (Ruiz Miguel, 2005: 135).

Yet, indirect forms of accountability consisted in declassifying or reveal secret documents. The regulation of this subject is based on the Official Secrets Act of 1968 (amended in 1978) and developed by a regulation of 1969. By those rules, it was possible to classify any issue as a secret by legislative or executive decisions. Thus, on the one hand, a material or document became official secret just by unilateral declarations suited to law. One example of those secrets is the mentioned "Reserved Funds". On the other hand, the Act required the protection of official secrets in any circumstance. It also demands to

[14] CESID functions appear in at least three regulatory measures. The first and more comprehensive is the Minister of Defense Order (135/1982), on which the Centre is demanded to supply "the information needs of the Prime Minister (...) on defense issues" as well of the Defense Minister on military policies. In addition to this order, the Royal Decree 1.883/ 1996 demands a coordinated action of the various organizations that used encoded procedures, as well as establishes the need for cryptographic security. Finally, the Royal Decree 2,632 / 1985, on "internal structure and relations" of CESID, modernizes the normative language (especially in the functions of domestic intelligence), and distributes the functions of CESID between the CEO and the various Intelligence Divisions (External, Interior, Counterintelligence, and Economics and Technology) (Revenga Sánchez, 2001: 63-65).

report civil or military authorities in case of findings. However, since there was not a regulation in cases of disobedience, those obligations were ignored in cases such as the "CESID papers" which revealed systematic violations of communication. By this case, the classified material came into the light "by the hands of unauthorized persons like bankers and journalists" (Ruiz Miguel, 2005: 142). Furthermore, the historian Goberna Falque, in his studies about the intelligence services in Spain, mentions several books that have been written as a result of official leaks or as conclusions of investigative journalism (Goberna Falque, 2005:25-74). These leaks represent the lack of answerability and enforcement dimensions. In addition, they could be deemed as informal ways that claim for an accountability project either through a vertical direction between the citizens and the State.

As the time passed, alternatives types of controls of surveillance activities have emerged. Regarding internal and vertical accountability, the executive branch has virtually been the most effective mechanism but also the worst regulated. The idea of security services as a sort of "technical and independent" organizations inside the Government is rejected by Ruiz Miguel. He infers that the CESID was configured as a dependant organization within the Executive branch, which in turn was responsible for the actions and consequences of the "Center" (Ruiz Miguel, 2005: 143).

More accountability dimensions have been asked by the Parliament. Nonetheless, this kind of control was incomplete as the Congress of Deputies faced restrictions to access and monitor surveillance practices. To overcome these obstacles, resolutions of 1992 have replaced, in a loose manner, a previous one from 1986 which was considered too restrictive. Despite the rules, the legislative control has continued in an inconsistent way. For instance, in 1995, when parliamentary observers tried to monitor the "Reserved Funds", they were supposed to request official secrets every semester. However, the Executive branch abandoned the obligation of semiannual accountability "ignoring the order to turn the government more accountable before parliament Commissions" (Ruiz Miguel, 2005: 145).

Finally, the CESID activities that collected personal information have been part of Judiciary supervision, including the case of Reserved Funds. In 1995, Madrid's magistrates required the disclosure of classified documents from the Ministry of Defense. After that, the Judiciary promoted a better control of surveillance activities (Ruiz Miguel, 2005). In part, this achievement was motivated by scandals after illegal interceptions of communications. Because of these violation, a Provincial Court revoked a previous decision that absolved the CESID' perpetrators and, in 1999, convicted them. This example represents answerability and, most important, enforcement within accountability, by a horizontal direction related to checks and balances.

Meanwhile, the clashes between the Executive and Judiciary branches concerning judicial interpretations were appeased when the Organic Law 4/1997 (the so-called Law of video surveillance) affirmed the

inviolability of the home and defended the secret of communications as parts of the generic guarantee to the right of privacy. Nowadays, any interference with these values must have a judicial authorization.[15] Jurists like Cano Bueso (1997) express that the judicial accountability has worked "satisfactorily". But at the same time, other authors such as Santolaya Machetti (1995) and Ruiz Miguel (2005) claim that a "satisfactory aspect" is questionable and, especially after the transformation of the CESID into the "National Intelligence Centre" (CNI), in 2002. The controls of the CNI are regulated by the Law 11/2002 and the Organic Law 2/2002. The former define the parliamentary commissions who have access to the strategies and budgets of the Agency. The latter define the judicial control over those actions affecting the secrecy of communication and the inviolability of the home. However, aside from juridical interpretations, more studies are needed to assess the accountability stemmed by these laws during the last years.

New surveillance assemblages

In the last decades, other forms of legacy constraints have risen due to surveillance practices. For instance, economic and international dynamics of globalization could be interpreted as critical junctures that affected the role of the States since the end of the last century (Horsman and Marshall, 1994; Weiss, 1998). Furthermore, the term "governance", or the act to establish web-like relations between public and private actors, has become a paradigm of our time. In the Spanish case, we can assure that state practices still matters and are a essential specially for informational and intelligence services. But since the transformation of the politics into an array of multi-level arenas and players –both at local and European levels or public and private spheres- the surveillance institutional borderlines have become blurred and their structures diffuse.

Today, personal information for surveillance purposes has an interest not only to the state protection or to monitoring radicalization and terrorism. It also shapes "normal" aspects of the contemporary life. In that sense, 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). Whereas vigilance has become more fragmented and decentralized, it opened a gate for establishing more horizontal accounting actions between the "watchers" and the "watched" (Haggerty and Ericsson, 2000: 611). Yet this interpretation can be questioned either by technological (Tsoukas, 1997) or

[15] Indeed, article 3 on this law regulates the installation of CCTVs in public areas. Besides that, there must be "an authorization given by a council headed by a magistrate, whose majority composition will not involve members of the Administration into question" (Revenga Sánchez, 2001: 77). But as shown in an empirical study led by Gemma Galdon Clavell, most of the times these authorizations are "automatized" and their real controls are very "loose" (Galdon Clavell et al., 2012: 60).

sociological approaches (Hier, 2003), its comprehension of the flows and "nomadic" aspects of vigilance is really essential.

The endeavors to track someone on the web are not separated from the physical world. Gaining access to those tracks and creating starting points for social control are still essential (although not only) to previous state bureaucracies and spies. Regardless the technological shifts and the interdependence of politics in governance, surveillance tasks are affected by a previous modus operandi (such as, secrecy and dissuasion) and by new security demands, especially on the internet. Therefore, even the digital personal data flows must be carefully considered and protected as they are fundamental parts representing individuals and social interactions in this century.

Personal data protection

Personal data protection was not initially mentioned in the Spanish Constitution but it is a fundamental right recognized by judicial terms. The Justice Law Sentence (STC) 253/1993 (and later regulations such as the Royal Decree 1720/2007) claimed personal data as a genuine fundamental right by its own content, both in negative and positive legal dimensions. Later on, the STCs 290/2000 and 292/2000 expressed the compatibility of personal data with constitutional backgrounds. The STC 254/1993 establishes several administrative points for the definition and implementation of personal data protection. By its Article 3, personal data is defined as the information that could be associated with a physical person. In that sense, it includes all types of data, whatever their format, presentation or evidence (voice, images, videos, fingerprints, genetic data, etc.). Whereas the same Article establishes file systems to store personal data, a controversial point emerges since the data could be mixed or fragmented, annulling the logic of a "sorted and structured information" (alphabetical, numerical, an order of arrival, code number, etc.) of the Article. In addition, the Sentence establishes a public or private organization which is be responsible for storing and protecting the data: the data controller. These organizations are of importance because they can be associated with the rights of data protection (access, rectification, cancellation and opposition). In addition, the data controllers need to establish coordination tasks with providers or intermediaries (data processors), which in turn can ensure access to data flows and work with this information after the consent of users (Articles10-15). Another milestone was the creation of the "Spanish Personal Data Protection Agency" (Agencia Española de Protección de Datos - AEPD) as this is the public authority responsible for implementing administrative sanctions and controlling public and private file systems in the Spanish territory.

In terms of accountability, the Agency (AEPD) is administratively statutory and hierarchically independent, and maintains contact with the Government through the Ministry of Justice. At the same time, its functions are addressed to receive citizen's petitions on data protection and to execute the rights related to this subject (access, rectification, cancellation and opposition). In addition, the Agency was

thought to promote external "answerability" of personal data systems and processors, including those systems stored by the police and security services (Article 22, Organic Law 254/1993). On the other hand, this control is not implemented when personal data issues hinder the fulfillment functions of public authorities, and when "National Defense, Public Safety, criminal and administrative prosecutions could be affected" (Article 23-4, Organic Law 254/1993). As this proceeds, the answers given by the legal framework are hampered in those cases when personal data is confronted with security issues (Guasch and Soler Fuensanta, 2015: 417). Besides that, accountability within the AEPD scope is limited due to its national jurisdiction and administrative range. Thus, other agencies on personal data were created inside the country, such as the Basque and Catalonian Personal Data Agencies, and abroad, as the "European Supervisor", whose tasks include, for example, personal data transfers and safeguarding of data processors lists in the European Union.

At the European level, the Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) recognizes the protection of personal data as an essential right:

> 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.[16]

Moreover, the European Parliament has produced several legislations on this subject. It is of importance the Directive 95/46/EC about the processing and transferring of personal data. Other milestones were the Directive 2002/58/EC on the protection of privacy and data in electronic communications; the Regulation (EC) 45/2001, which allowed the creation of the "European Data Protection Supervisor" (EDPS) as the authority (consultation and cooperation) responsible that independent institutions and organizations inside the Union perform theirs obligations regarding data protection. The Decision 2008/977 (Council on Justice and Interior Affairs) also regulates the protection of personal data processed in the framework of police and judicial cooperation as well as in the criminal area. This Decision regulates data protection in accordance with the previous "third pillar" of the Union and it is only applied to the police and to judicial data exchanges between the Member States, authorities and systems of the UE (without the inclusion of national data sources). In the "Area of Freedom, Security and Justice" (AFSJ) –which is the front of the EU regarded to security and surveillance practices- the main systems among the Member States to collecting personal data are the Schengen Information System

[16] Charter of Fundamental Rights of the European Union. Official Journal of the European Communities. 12/2000. Accessible at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf, access date 08/02/2016.

(SIS), the Customs Information System (SIA), the Information Visas System (VIS) and the European Police Agency or EUROPOL.

Accountability efforts and their limits

As mentioned above, public and private institutions, both at Spanish and European levels, pursued mechanisms to protect privacy through the protection of personal data. Consequently, it was deemed that information in this scope should not serve for disproportional measures and deregulated goals in the hands of political/economic powers. In that sense, personal data protection is a new form of accountability involving both answerability and enforcement as it defines data rules which restraint surveillance over "all aspects" of our digital lives. Nevertheless, in a time when being exposed and seeing the others disseminate a synoptic metaphor of surveillance (where the few are being seen by the most), it could be easy to perceive our time as a period of more freedom and transparency, especially in democratization contexts. However, this kind of transparency, the one where individuals are seen by multiple audiences (Byung-Chul, 2012), could mislead the comprehension of other surveillance dimensions. That is, one considerable obstacle to accountability in today's democracies comes from that a "transparency world" does not necessarily imply in deep and external controls over the surveillance processors, such as over security forces and private agencies.

Moreover, whether accountability needs to be related to external controls (in horizontal and vertical directions), this project is jeopardized by a sort of generic narratives about responsibility and values that are in vogue instead of a real internalization of those narratives and institutionalized supervisions. This statement can be attested when we appreciate the evolution of the data protection right in the EU. The EU began by recognizing the right to data protection (privacy, dignity) as a general principle of Common Law, and incorporated it to the jurisprudence of the "European Court of Human Rights" (ECHR) as well as of the "Court of Justice of the European Union" (CJEU). That is, to check the "proportionality" and justification of the cases that could interfere with those rights, the jurisprudence is supposed to be a mechanism to supervise and, theoretically, to enforce and turn accountable those activities that process personal data (including surveillance practices). The Jurisprudence also tried to reinforce the roles played by data protection Agencies both at national and European levels. 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 (Arena Ramiro, 2011).

Other kinds of thresholds to accountability 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). Though, 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 on the personal data transfers to other 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). Finally, other attempt to turn personal data processors more accountable was made in 2014. At this time, "Google Spain" and the AEPD clashed about the so-called "right to be forgotten". As a result, the Agency established that the manager of a web search engine is also responsible for processing personal data even when the content is published via third parties (Silva de la Puerta, 2014). All the same, we must underscore that a set of external controls has been deployed, especially through legal standards and in some cases by enforcement dimensions. Yet, there are many fronts on this field, specifically promoted by the "third dimension" or international direction of accountability. The so-called "privacy by design" and the "General Data Protection Regulation" (GDPR) to be implemented at the European level in 2018 is a paradigmatic change that must be carefully introduced and checked.

The cases above suggest that accountability was performed through juridical "clashes" rather than to an institutionalized effort with permanent controls and external supervisions. Those clashes can be understood as critical junctures that reoriented and promoted accountability mechanisms in spite of the legacy constraints and the lack of an overall framework to protect data and privacy. Thus, personal data protection rights usually are defended "a posteriori" and they are also reduced to an individual context, especially when their lines are pushed back when they face "untouchable" aspects of surveillance practices (such as a certain level of secrecy). Nonetheless, it is worthy to mention that despite the limits of accountability, there are many areas that could be improved in further analysis and studies. And this articles cannot close its lines without mentioning some objects for coming efforts, such as: a) the lack of distinction and the ambiguous definition of "personal data" in the sense that "data" relies on a logic criteria to be stored and on persons although the fragmentation and anonymity on the internet; b) the need to define clearly new categories for international data transfers and data protection, such as in the management of "genetic data"; and c) the need of creating new standards of "transparency", "responsibility" and "accountability" in several legal frameworks. The last point is really essential since there is a relatively weak role of national data protection authorities and a lack of evaluation of data protection in criminal prosecution, police and justice cooperation within the European Union.

Conclusion

Although there are several frameworks and practices about surveillance practices, a clear point arises when it comes to the procedures that collect personal information: the decentralization of this practice from the State's hands. In the Spanish case, which emerged from an authoritarian period, surveillance practices and accountability efforts in this area were analyzed in two periods. While the first period was focused on Spanish institutions of espionage since the late 70s, the second one was related to technological flows of personal data and its control since the advent of the web in the last two decades. In the first period, the accountability efforts are related to the classical "check and balances" or horizontal directions among political branches (Executive, Legislative and Justice). In the last period, a new form of independent institutions and accountability, a sort of ombudsman figures, were created to promote and ensure the rights associated with the protection of personal data (privacy, dignity, access to personal data plus rectification and opposition). The examples of this study depicted the external controls that were deployed over the main internal surveillance institutions and the creation of new fronts to regulate a complex digital information network, as in the case of the "Spanish Agency for Protection of Personal Data" (AEPD).

However, the accountability efforts, either by "classic" or new and independent mechanisms, have been affected in terms of its quality and its mechanisms, especially in the face of past institutions like the SECED and the CESID in the first period. The legacy constraints stemmed from those institutions and their secrecy, as stated by this research and by the bibliography, have jeopardized the accountability mechanisms to a limited scale, especially when it comes to promote stronger supervisions and to foster enforcement dimensions. In the last period of the analysis, non-governmental and private actors have been inserted into an array of informational arenas, either for surveillance purposes or for actions that could be linked to surveillance capabilities. And in order to maintain democratic controls over the old and new/potential actors in this field, constitutional states like Spain have considered mechanisms beyond the governmental and institutional lines. As a result, there were created rules to ensure personal data rights. Nevertheless, those rights have been protected by posteriori measures of answerability and by uncoordinated efforts of enforcement. Therefore, it seems that the gaze must also be turned beyond a concept of personal data embedded in an individual and micro level as this change can help to create further enforcement dimensions in a new and diffuse surveillance.

Moreover, the decentralization of the informational power on the stronger side –the state and other stakeholders– has led to the fragmentation of attentions on the weaker side –the citizens–, as suggested by Raab (2013). As the malleability of power increases, especially by digital trends, it blurs our apprehension of surveillance assemblages and our capacity to demand accountability related to privacy and data. Hence, whenever is possible, it is of importance to oversight the implicit and dynamic

surveillance practices and the opportunities to restraint them. For instance, vertical directions of answerability asked by citizens over their own data and new technological designs can spark enforcement dimensions even in a relation marked by asymmetry of powers. Moreover, they cannot be forsaken at the expense of legal and stronger mechanisms of accountability. In that sense, the Spanish case has shown that from previous "Janus" filing systems to the internet flows of today, accountability must be aware of direct and implicit surveillance practices handled by state and non-governmental actors. For those reasons, accountability mechanisms still must be rethought and replenished in the current surveillance scenarios.

References

Aba Catoria, A. (2002). "El secreto de Estado y los servicios de inteligencia". Cuadernos Cons. de la Cátedra Fadrique Furió Ceriol n. 38/39. Valencia, pp. 133-168.

Arena 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.

Bauman, Z. (1998). "Globalization: The Human Consequences". New York: Columbia University Press.

Boersma, K.; Ságvári, B. and Backman, C. (2011). "Living in Surveillance Societies: The Ghosts of Surveillance". Proceedings of LiSS Conference 2, Editura Universităţii, Iasi.

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

Cano Bueso, J. (1997). "Información parlamentaria y secretos oficiales". Revista de las Cortes Generales 42, pp. 30-34.

Caluya, G. (2010). "The post-panoptic society? Reassessing Foucault in surveillance studies". Social Identities Vol. 16, No. 5, September 2010, pp. 621-633. https://doi.org/10.1080/13504630.2010.509565

Collier, R. B., & Collier, D. (2002). Shaping the political arena (p. 53). Notre Dame, IN: University of Notre Dame Press.

David, P. A. (2007). "Path dependence: a foundational concept for historical social science". Cliometrica, 1(2), 91-114. https://doi.org/10.1007/s11698-006-0005-x

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

Díaz Fernández, A. M. (2005). "El servicio de inteligencia: un actor político en la transición española". Stud. hist., H.ª cont., 23, Universidad de Salamanca, pp. 201-219.

Díaz Fernández, A. M. (2006). "El servicio de inteligencia español a la luz de la teoría de la organización". Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol n. 48, pp. 19-39.

Diken, B. and Laustsen C. B. (2002). "Zones of indistinction: security, terror, and bare life". Working Paper, Department of Sociology, Lancaster: Lancaster University.

Foucault, M.(2014). "Surveiller et punir, Naissance de la prison". Paris: Editions Gallimard.

Galdon Clavell et al. (2012). "CCTV in Spain: An empirical account of the deployment of video surveillance in a Southern-European country". Information Polity 17, pp. 57-68.

Goberna Falque, J. R. (2005). "Los servicios de inteligencia en la historiografía española". Arbor CLXXX, 709, Enero 2005, pp. 25-74. https://doi.org/10.3989/arbor.2005.i709.497

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.

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

Guasch Portas, V. and Soler Fuensanta, J. R. (2015). "El interés legítimo en la protección de datos", Revista de Derecho UNED, 16, 2015, pp. 417 & ss. https://doi.org/10.5944/rduned.16.2015.15245

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.

Hier, S. P. (2003). "Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control". Surveillance and Society 1(3), pp. 399-411.

Horsman, M. and Marshall, A. (1994). "After the nation-state: citizens, tribalism and the new world disorder". London: Harper Collins.

Huntington, S. (1994). "A terceira onda: a democratização no final do século XX", São Paulo: Ática.

Immergut, E. M. (2006). "Historical institutionalism in political science and the problem of change". In Understanding Change (pp. 237-259). Palgrave Macmillan UK. https://doi.org/10.1057/9780230524644_17

Los, M. (2006). "Looking into the future: surveillance, globalization and the totalitarian potential", in Lyon, David (ed.), Theorizing surveillance: the panopticon and beyond, Cullompton: Willan Publishing.

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

Mathiesen, T. (1997) "The Viewer Society", Theoretical Criminology, Vol 1(2), Sage Publications, London. https://doi.org/10.1177/1362480697001002003

McCahill, M. (2001). "The Surveillance Web: The Rise of Visual Surveillance in an English City". Devon: Willan Press.

Norris, C. and G. Armstrong (1999). "The Maximum Surveillance Society: The Rise of CCTV". Oxford: Berg.

Peñaranda Algar, J. M. (2005). "Los servicios de inteligencia en la transición". Arbor CLXXX, 709, Enero 2005, pp. 99-119. https://doi.org/10.3989/arbor.2005.i709.499

Pierson, P., & Skocpol, T. (2002). "Historical institutionalism in contemporary political science". Political science: The state of the discipline, 3, 693-721.

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.

Revenga Sánchez, M. (2001). "Servicios de inteligencia y derecho a la intimidad". Revista Española de Derecho Constitucional, 21, N. 61. Enero-Abril, pp. 61 ss.

Rhodes, R.A.W. (1997). "Understanding governance: policy networks, governance, reflexivity and accountability", Maidenhead, Philadelphia: Open University Press.

Ruiz Miguel, C. (2005). "El CESID: Historia de un intento de modernización de los servicios de Inteligencia". Arbor CLXXX, 709, Enero 2005, pp. 121-150. https://doi.org/10.3989/arbor.2005.i709.500

Santolaya Machetti, P. (1995). "El control de los Secretos de Estado; la experiencia en Derecho comparado", Poder Judicial 40, pp. 57-73.

Samatas, M.; Frois, C. and Galdon Clavell, G. (2011). "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils

Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2, Editura Universităţii, Iasi.

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.

Steinmo, S. (2008). "Historical institutionalism". Approaches and methodologies in the social sciences: A pluralist perspective, 118-138. https://doi.org/10.1017/CBO9780511801938.008

Tsoukas, H. (1997). "The tyranny of light: Temptations and the paradoxes of the information society". Futures, Vol. 29, N.9, pp. 827-843. https://doi.org/10.1016/s0016-3287(97)00035-9

Weiss, L. (1998). "The myth of the powerless state. Governing the economy in a Global era", Cambridge: Polity Press.

Yar, Majid (2003). "Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis". Surveillance and Society 1 (3), pp. 254-271.

Zorzo Ferrer, F. J. (2005). "Historia de los servicios de inteligencia: El periodo predemocrático". Arbor CLXXX, 709, Enero 2005, pp. 75-98. https://doi.org/10.3989/arbor.2005.i709.498