From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France

Félix Tréguer*
felix.treguer@sciencespo.fr

October 2016†

Abstract

Taking France as a case-study, this working paper reflects on the ongoing legalization strategies pursued by liberal states as they seek to secure the Internet surveillance programs operated by their domestic and foreign intelligence agencies. Following the path to legalization prior and after the Snowden disclosures of 2013, the paper shows how these leaks helped mobilize contentious groups against the extra-judicial surveillance of Internet communications, a policy area which had hitherto been overlooked by French human rights advocacy. It also points to the dilemma that post-Snowden contention created for governments. On the one hand, the disclosures helped document the growing gap between the existing legal framework and actual surveillance practices, exposing them to litigation and thereby reinforcing the rationale for legalization. But on the other hand, they made such a legislative reform politically risky and unpredictable. In France, policymakers navigated these constraints through a cautious mix of distinction strategies, silence, and securitization. After the Paris attacks of January 2015 and a hasty discussion in Parliament, they eventually passed the Intelligence Act –the most extensive piece of legislation ever adopted in France to regulate secret state surveillance. The paper concludes by pointing to the paradoxical effect of post-Snowden contention: French law now provides for clear rules authorizing large-scale surveillance, to a degree of detail that was hard to imagine just a few years ago.

*Félix Tréguer is a junior researcher at CERI-Sciences Po where he works on communications surveillance for the UTIC project (coordinated by Didier Bigo and funded by the French National Research Agency). He is also a PhD student at EHESS. His research focuses on past and present contention around the protection of civil rights and communicational autonomy on the Internet. Disclaimer: Félix is a founding member of the Paris-based digital rights advocacy group *La Quadrature du Net* and is involved in the *Exégètes Amateurs*, a team of volunteers working on strategic litigation against Internet censorship and surveillance.

†This document is an updated version of the working paper presented at the 7th Biennial Surveillance & Society Conference in Barcelona, Spain, on April 22nd, 2016.

DRAFT

Write to the author for any comment, question, correction, criticism.

Download the latest version at the following address: http://is.gd/9ickne

Contents

Introduction

In January 2008, a meeting took place in the office of then-President of France, Nicolas Sarkozy, at the Élysée Palace. In front of him sat Prime Minister François Fillon and the Director of the *Direction générale de la Sécurité extérieure* (DGSE, France's foreign intelligence agency) Pierre Brochand, as well as a few of their staff.

Brochand had come with a plea. France, he explained, was on the verge of loosing the Internet surveillance arms race. From the 1980's on, French intelligence services had managed to develop top-notch communications intelligence (COMINT) capabilities, thanks to a network of intercept stations located across metropolitan France and overseas territories (sometimes in partnership with the German *Bundesnachrichtendienst*, or BND).[1] But as almost all of the world's communications were now travelling on IP-based networks, the DGSE was loosing ground on its main partners and competitors. Since 9/11, the National Security Agency (NSA), the British Government Communications Headquarters (GCHQ) and the wider Five-Eyes networks of Anglo-Saxon COMINT agencies had poured billions of dollars to scale up their Internet surveillance programs. The DGSE had not.

[1] Vincent Jauvert. *Le DGSE écoute le monde (et les Français) depuis plus de trente ans*. NouvelObs.com. July 4, 2013. Available at: http://globe.blogs.nouvelobs.com/archive/2013/07/04/comment-la-france-ecoute-le-monde.html.

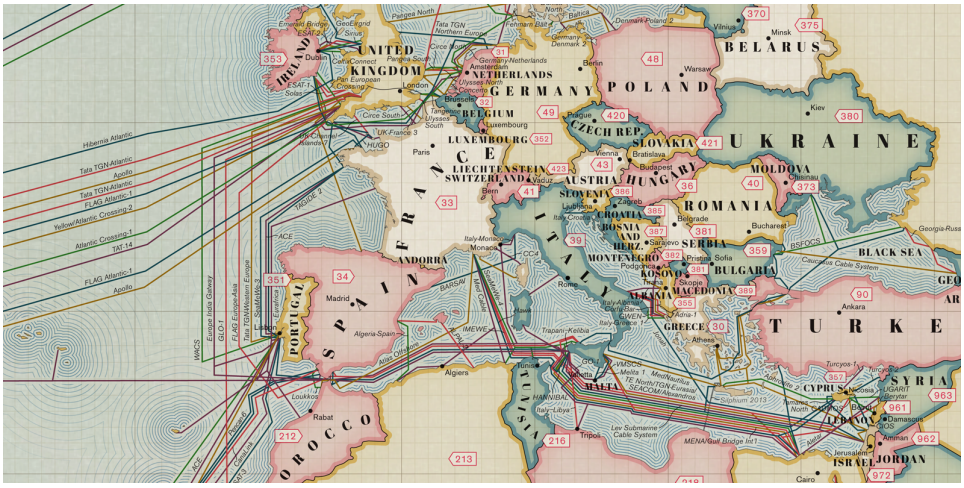

Figure 1: Location of France in the international network of submarine cables (Telegeography, 2013).

France had some serious catching-up to do. But it also had important assets. First, its geographic location, with almost two dozens of submarine cables landing on its shores, both in Brittany, Normandy and the Marseilles area (see figure 1). Second, its engineering elite state schools and high-tech firms –not least of which submarine cable operators Alcatel and Orange as well as surveillance technology provider Qosmos–, which could provide the technical know-how necessary to carry on this ambitious project.[2]

Sarkozy was hesitant. The plan was very costly and its legality more than dubious. The French legal basis for communications surveillance dated back to 1991, when after a condemnation by the European Court of Human Rights (ECHR), the Parliament adopted a law to legalize telephone wiretapping and give a blank check to the DGSE to conduct satellite and other forms of wireless interceptions[3]. Another issue was that of cost. At the time, the 2008 financial crisis had yet to unleash, but the government was already facing recurring deficits and it needed to contain public spending.

But Pierre Brochand and its supporters in the President's staff turned

[2]From 2011 on, the French Strategic Investment Fund also invested dozens of millions of euros in companies like Qosmos, Bull and Ercom to promote and protect French know-how in traffic analysis and Big Data security applications. *Le FSI épaule les grandes oreilles*. Intelligence Online. Sept. 29, 2011. Available at: http://www.intelligenceonline.fr/intelligence-economique/2011/09/29/le-fsi-epaule-les-grandes-oreilles,93184212-ART-HOM; On the collaboration between Qosmos and the DGSE, see: Franck Johannès and Simon Piel. *"Kairos", le lien public-privé du renseignement français*. Le Monde.fr. Oct. 28, 2013. Available at: http://www.lemonde.fr/societe/article/2013/10/28/qosmos-collabore-avec-le-renseignement-francais_3503940_3224.html.

[3]*Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.*

out to be convincing. The geopolitical context was also somewhat "favorable." In Mauritania, four French citizens had just been killed by islamic militants from al-Qaeda in the Islamic Maghreb, an organization which was fast growing in Northern Africa and represented mounting threat against French interests.

Sarkozy eventually agreed to move forward with the proposed plan. Over the course of the next five years, the DGSE would get the €700 million it needed to upgrade its surveillance capabilities and hire over 600 staff to work in its technical Directorate (the number of DGSE employees was then 4 440).[4] Only six months later, near Marseilles, the first of the new intercept stations was up and running, doubling up the traffic coming from international cables, filtering it and transmitting it to the DGSE's headquarters in Paris.

Sarkozy had also instructed that a legal basis be found to back up the scheme, but in secret so as to keep the plan out of the sight of public opinion as well as of France's adversaries and competitors in the intelligence world. This proved to be a little more tricky that it had first seemed.

But the DGSE and the oversight commission –then named *Commission nationale de contrôle des interceptions de sécurité* (or CNCIS, established by the 1991 law)– eventually came to a agreement over the secret rules that would govern the large-scale interception of Internet traffic. One of them provided for instance that communications between French residents should immediately be deleted from the DGSE's databases. Another allegedly forbade the DGSE to use these new tools to spy on political or economic interests of other European Union member states.

How do we even know about this meeting? We owe this account to journalist Vincent Jauvert, who revealed its existence in a French weekly magazine on July 1st, 2015, at the very end of the parliamentary debate on the 2015 Intelligence Bill.[5]

According to former high-ranking officials quoted by Jauvert, these efforts paid back: "When we turned on the faucet, it was a shock!. All this information, it was unbelievable!" All of sudden, France was back in the game. To such an extent that, a few months later, in 2009, the NSA even offered to make the DGSE a member of the exclusive Five-Eyes club.

Apparently, the "Sixth Eye" deal failed over the CIA's refusal to conclude a no-spy agreement with France. In 2011, a more modest cooperation was eventually signed between the NSA and the DGSE under the form of a

[4] Didier Boulaud. *Avis n°94 sur le projet de loi de finances pour 2008 (Défense - Environnement et soutien de la politique de défense)*. Paris: Sénat, Nov. 22, 2007. Available at: http://www.senat.fr/rap/a07-094-7/a07-094-74.html, p. 21.

[5] Vincent Jauvert. *Comment la France écoute (aussi) le monde*. L'Obs. July 1, 2015. Available at: http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html.

memorandum –most likely the so-called LUSTRE agreement revealed in 2013 by NSA whistleblower Edward Snowden.[6] Another agreement with the British GCHQ was struck in November 2010.

Jauvert's report connected many pieces of information of what was –and still remains– a puzzle. By then, a few public statements by intelligence officials had already hinted at the formidable growth of the DGSE's Internet surveillance capabilities. The Snowden documents and a handful of investigative reports had also given evidence of France's rank in the world of COMINT. However, for the first time, we were able to get a sense of some of the political intricacies and "deep state" negotiations that presided over the rise of the most significant Internet surveillance program developed by French agencies, as well as their geopolitical outcomes.

But if the plan agreed upon at the Élysée Palace in January 2008 was so successful, why did the new French administration elected in the Spring of 2015 chose to "go public" by presenting the Intelligence Bill? By 2008, it was clear to many in government that the French legal basis for surveillance needed some serious updating. But a mixture of national security imperatives and advocacy failures allowed these illegal programs to escape public notice. After June 2013, however, the convergence of "post-Snowden" contention and securitization produced a perfect storm that made the legalization of previously illegal practices both unavoidable and politically doable.

The goal of this paper is to study this process of *legalization*, taking France as a case-study to analyze the impact of post-Snowden contention on techno-legal apparatus of surveillance that have become deeply embedded in the daily routine of security professionals, both in the domestic and transnational security fields. To that extent, it seeks to contribute to cross-country comparisons of post-Snowden contention.

Through legal analysis and by mobilizing the methodological toolbox of contentious politics,[7] it provides a historical overview of the legalization process of French COMINT activities, before delving on the impact of both the Snowden disclosures and ensuing civil society mobilizations on this process, paying particular attention to the adoption of the Intelligence Act of 2015.

[6] According to Jauvert's sources, the NSA-DGSE memorandum provided for the real-time sharing of intelligence regarding terrorism and nuclear proliferation as well as sharing of metadata coming from countries like Syria and Iran, plus a cooperation in decryption capabilities. Press reports based on the Snowden documents have since provided information regarding the volume of data-sharing, asserting that from December 10th 2012 to January 8th 2013, the DGSE handed over 70 million metadata records to the NSA (Jacques Follorou. *Surveillance : la DGSE a transmis des données à la NSA américaine*. Le Monde.fr. Oct. 30, 2013. Available at: http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html).

[7] In particular, we will seek to emphasize antecedents and consequence of contentious episodes around surveillance, conduct content analysis of parliamentary debates and examine networks of contentious actors. Charles Tilly and Sidney Tarrow. *Contentious Politics*. 2nd edition. New York: Oxford University Press, 2015. 288 pp.

The paper concludes by suggesting that, rather than helping restore the rule *of* law, post-Snowden contention might paradoxically contribute to reinforcing illiberal trends towards the circumvention of procedural and substantive human rights safeguards, while strengthening the executive power's ability to "rule *by* law."[8]

1 Before Snowden, Legalization Was Underway

Before looking at post-Snowden contention, this sections offers a historical overview of anti-surveillance contention and legalization processes. We start by looking past scandals and then look at intelligence reform and legalization framing in the run-up to the Snowden disclosures.

1.1 A Record of Surveillance Scandals

Like in other liberal regimes, scandals involving secret state surveillance have played a significant role in shaping the French legal regimes and practices in the fields of communications intelligence and privacy.

The SAFARI affair

One major episode of anti-surveillance contention occurred just as the United States were also embroiled in various scandals –from the stunning revelation of then FBI's COINTELPRO domestic surveillance program to the Watergate.[9] On March 21st, 1974, the French daily *Le Monde* ran a story revealing that the ministry of the Interior was working on a centralized system interconnecting all the databases held by some of the biggest public administrations (law enforcement agencies, the ministries of Justice and Labor, the army, welfare services, etc.). The system was to be based on a powerful computer developed under a public research program, the Iris-80.

In his article, *Le Monde*'s reporter, Philippe Boucher –who apparently got the story from a computer engineer turned whistleblower–[10] was stunned to discover that the whole project had been veiled in secrecy, and that the government had sought to bypass the Parliament. "We have every reason to doubt the purity of this endeavour," he wrote, "considering how much care is given to conceal its implementation."

[8] Sidney Tarrow. *War, States, and Contention: A Comparative Historical Study.* 1 edition. Ithaca ; London: Cornell University Press, 2015. 328 pp., p. 162.

[9] These scandals that marked the presidency of Richard Nixon led to a major Congress investigation with the Church Committee and the adoption of the Foreign Intelligence Surveillance Act in 1976.

[10] Here, we rely on the account of Louis Joinet, the first President of the French data protection authority, the *Commission nationale informatique et libertés* (CNIL). See: Louis Joinet. *Mes raisons d'État: Mémoires d'un épris de justice.* La Découverte, 2013. 331 pp.

• • • LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grappillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un « identifiant », qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

« Safari » ou la chasse aux Français

Rue Jules-Breton, à Paris-13e, dans des locaux du ministre de l'intérieur, un ordinateur Iris-80 avec bi-processeur est en cours de mise en marche. A travers la France, les différents services de police détiennent, selon la confidence faite par un très haut magistrat, 100 millions de fiches, réparties dans 400 fichiers. Ainsi se trouve posées — et, à terme, théoriquement résolues — les données d'un problème comprenant, d'une part, l'énormité des renseignements collectés ; de l'autre, la méthode à définir pour faire de cet ensemble une source unique, à tous égards, de renseignements.

L'histoire du très puissant appareil qu'est l'Iris-80 est exemplaire du secret qui entoure l'épanouissement de l'informatique dans les administrations, quelles que puissent être les informations qui filtrent ici et là.

Puissant, cet Iris-80, une comparaison le démontre sans contestation. L'appareil employé pour engranger les données de l'opération Safari, qui concerne l'identification individuelle de l'ensemble des 52 millions de Français, a une contenance de 2 milliards d'octets (1) ; celle de l'ordinateur du ministère de l'intérieur est de 3,2 milliards d'octets.

l'origine, budgétairement, n'était pas du tout prévu pour la tâche qu'il a finalement assurée, mais pour « traiter » les données administratives du Fichier national des constructeurs (F.N.C.). Il s'agit donc apparemment d'un détournement manifeste de crédits d'études, ce qui n'était sans doute pas le vœu du Parlement qui les vota.

De vastes ambitions

Il n'y a pas que cela. Le ministère de l'intérieur a d'encore plus vastes ambitions. Détenteurs, déjà, du fichier national du remembrement, les services de M. Jacques Chirac font de grands efforts pour, affirme-t-on, s'en adjoindre d'autres : le cadastre, le fichier de la direction nationale des impôts et, plus grave peut-être, celui du ministère du travail.

De telles visées comportent un danger qui saute aux yeux, et que M. Adolphe Touffait, procureur général de la Cour de cassation, avait parfaitement défini le 9 avril 1973 devant l'Académie des sciences morales et politiques, en disant : « *La dynamique du système qui tend à la centralisation des fichiers risque*

Ce n'est pas, pourtant, que les avertissements aient manqué. Le Conseil d'État en 1970, puis le ministère de la justice en 1972 (qui avait rappelé le rôle dévolu à l'autorité judiciaire de « gardien des libertés individuelles » et donc réclamé voix au chapitre) ont insisté sur la nécessité d'une intervention législative qui préciserait les quelques éléments essentiels de l'emploi de l'informatique appliquée aux particuliers : réglementation de l'accès des tiers aux fichiers, de l'intercommunication de ceux-ci, droit de rectification des personnes fichées si les renseignements retenus sont inexacts, etc.

De plus, tous les exemples étrangers incitent à ce débat sur une utilisation de l'informatique à laquelle, par définition, il ne s'agit pas de renoncer, mais à qui doivent être tracées des limites, si grand est le danger qu'elle implique. La désignation par le gouvernement d'une commission de « sachants » dans les semaines à venir ne saurait suffire à remplacer le débat parlementaire dont on se méfie si visiblement.

En fait de débats parlementaires, il y a d'ailleurs des précédents qui sont le fait, précisément, du minis-

outil, il n'apparaît pas — sauf erreurs négligeables, relativement — que l'accès des tiers ou le droit à contrôle des personnes visées — par demande d'un extrait — ait jamais provoqué des bavures préjudiciables à la légalité.

De même, le fichier national des conducteurs, dans sa partie judiciaire, est prévu par une loi, et il faut regretter que les textes d'application ait permis des illégalités injustifiables — mais connues (*le Monde* du 8 mars).

« A la hussarde »

Fort, pourtant, de ces avantages, le ministère de la justice paraît curieusement se laisser dépasser par des querelles internes peu compréhensibles. L'arrêté signé le 18 mars par M. Jean Taittinger le montre. La création d'une « division de l'informatique », place Vendôme, serait en soi une bonne chose, du point de vue de l'efficacité, si les conditions de sa création, engagée vraiment voici trois mois, ne prenait l'allure d'une peu élégante tentative d'élimination dirigée contre certains esprits novateurs ayant eu le mauvais goût de s'intéresser trop tôt à l'informatique.

dite commission. D'autant qu'il est d'ores et déjà connu que M. Touffait a été rayé de la liste des « sachants ». Il semble d'ailleurs que les réactions vives qui sont enregistrées portent moins sur le renouvellement des structures, jugées inévitables, que sur la méthode « *à la hussarde* » employée par tel membre de l'entourage de M. Taittinger pour mener à bien ses projets de rénovation de la gestion dans le domaine judiciaire.

Est-ce à dire de plus que les choix que l'on entend promouvoir soient nécessairement les plus opportuns ? Tout indique, pour l'instant, que, si le ministère de l'intérieur a définitivement choisi le « matériel lourd » pour s'équiper, la chancellerie, au contraire, s'oriente vers un réseau de mini-ordinateurs placés auprès de chaque tribunal de grande instance important.

Dans cet ordre d'idée, le choix déjà décidé de M. Jean Malbec, vice-président à Bobigny (Seine-Saint-Denis), comme futur chef de la division de l'informatique (au point qu'il a, dès à présent, effectué des missions d'information à Lille, Nice, Lyon et Marseille dans les semaines passées), est significatif. Il est, en effet, à Bobigny l'apôtre d'un sys-

d'un aggiornamento technique, a illustré son discours par un large reportage sur les équipements du tribunal de Bobigny — plus réduits, donc plus rapides à réaliser, ainsi plus vite source d'orgueil pour leurs créateurs.

C'est donc un doute global qui pèse sur les intentions du gouvernement, en général, et du ministère de la justice, en particulier : ce dernier département, qui rappelle à tous sa mission de protection des libertés individuelles, a apparemment accepté sans broncher la suppression d'un éventuel débat public, ce qui jette sur les déclarations « libérales » de M. Taittinger en d'autres domaines une suspicion qui n'est pas de bon aloi.

Mais, dans cette entreprise, le ministère de la justice, même s'il fait preuve d'une grande mollesse pour la défense de ses idéaux, car il ne s'agit pas seulement à présent de « *protéger des délinquants* », n'est pas essentiellement en cause. Ce qui l'est, c'est une entreprise dont on a tout lieu de suspecter la pureté tant on prend soin de cacher sa réalisation.

PHILIPPE BOUCHER.

Figure 2: Capture of *Le Monde*'s report on the SAFARI program (March 21st, 1974).

At the time, the memory of World War II and of the abuse of the Vichy government were still vivid, and the revelation stirred an important controversy about the dangers of computer surveillance. Facing a growing scandal, the government chose to withdraw the plan. But it did more than backtracking: It went on to commission a report on the protection of civil rights in the age of computing. The so-called Tricot report, published in 1977, voiced what were then widespread concerns: "By reinforcing the means of the government to track, analyze and expose various human activities," the report stressed, "computers go in the direction of technical efficiency but not that of liberty."[11]

The following year, the French data protection law –the so-called *loi "informatique et libertés"*– was adopted, establishing a data protection authority with significant powers on both public and private databases –although in the name of "national security," those of intelligence services remained out of its reach.[12] At the time, as in other countries undergoing similar reforms, the debate helped underline the profound ambivalence of computers. And so that same year, another law was adopted to promote transparency

[11] Quoted in: *De Safari à Edvige : 35 années d´une Histoire oubliée malgré la création de la CNIL*. Mag-Securs. Feb. 8, 2009. Available at: http://www.mag-securs.com/news/articletype/articleview/articleid/23700/de-safari-a-edvige--35-annees-d8217une-histoire-oubliee-malgre-la-creation-de-la-cnil.aspx.

[12] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

of public administrations and the right to information.[13]

The outcome of the SAFARI affair thus strongly contrast with post-Snowden contention: In this period of significant progress for the rule of law, computer technologies were met with legal innovations aimed at creating new constraints for the government, by inhibiting its ability to spy on its citizens and imposing increased openness to state bureaucracies.

The 1991 Wiretapping Act

The next important reform of the "surveillance *versus* privacy" debate happened more than a decade after the SAFARI affair. Back then, France lacked any specific statute to regulate the wiretapping of telephone calls. In the 1970's, there had been several attempts by member of the Parliament to create an oversight commission for administrative wiretapping, which was known to be routinely practiced under the authority of the Prime Minister. Each time, these attempts were met with rebuttal from the executive branch. In 1973, a member of the government, Olivier Stirn, even argued before the National Assembly that a law was useless:

> All in this area relies upon the conditions of execution and authorization; that is to say, ultimately, in the trust that, regardless of their political opinion, citizens of a democratic state must place in their government."[14]

Questions regarding the lack of appropriate legal framework would often resurface. In 1981 for instance, the new Socialist government sought to distinguish itself from its predecessors, and commissioned a report on wiretapping and the balance between crime prevention and *sûreté de l'État* on the one hand, and civil rights on the other.[15] Among other things, the report called for the adoption of a law to provide new criminal sanctions against illegal secret surveillance and the creation of an oversight commission. It was immediately shelved by the government and would only be published a decade later, just before the burst of another surveillance scandal involving the secret surveillance carried at the Élysée palace from 1983 to 1986 under the authority of President François Mitterrand.

Even for telephone surveillance conducted for criminal investigations, there was no specific law. Judicial wiretaps were then authorized under

[13] *Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.*

[14] Quoted in: Roger Errera. "Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques". *Revue trimestrielle des droits de l'Homme* 55 (2003), pp. 851–870, p. 853.

[15] Errera, "Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques", p. 856.

a broad provision defining the investigatory magistrate's authority (*juge d'instruction*). It covered "all acts of investigation he deems useful to the manifestation of the truth."[16].

Legal experts knew very well that the existing framework failed to meet the test of Article 8 of the European Convention of Human Rights (ECHR) –at least as it had been interpreted since th mid-1980's. The Court's case law was clear: For any interference by public authorities in the private lives of their citizens to be compliant with the Convention,

> the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.[17]

With this progressive case-law, important criminal cases from France eventually reached the ECHR. And in two unanimous decisions issued in April 1990,[18] the Court eventually struck down French wiretap warrants for they were not carried on "in accordance with the law."

In response to these condemnations, the government moved quickly to enact a statute covering both judicial and administrative wiretapping of "*correspondances*," that is to say the content of private communications. After only forty days of legislative debates, the Parliament passed the Wiretapping Act of 1991. From now on, judicial wiretaps could only be ordered by the investigatory magistrate, only when necessary and for serious crimes punished by more than two years of imprisonment, and with many procedural safeguards (written decision, record-keeping, special protections for lawyers, etc.).

As for administrative wiretaps conducted by intelligence services on the French territory –which the law called "security interception"–, they could be allowed "exceptionally" and only for the following goals: national security, the safeguarding of France's "scientific and economic potential," the prevention of terrorism, organised crime and reforming of extremist groups and militias that had previously been dissolved (in application of a law of January 10$^{\text{th}}$, 1936 against fascist leagues). Wiretap authorizations were issued under the authority of the Prime Minister for a renewable 4-month period.

Finally, an administrative oversight commission was established. Named *Commission nationale de contrôle des interceptions de sécurité* (CNCIS), it comprised nine members, both magistrates and members of Parliament. The

[16] Article 81(l) of the Code of criminal procedure.

[17] ECHR, *Malone v. United Kingdom*, n° 8691/79 , 26 April 1985.

[18] ECHR, *Kruslin v. France*, n° 11801/85, 24 April 1990 ; ECHR, *Huvig v. France*, n° 11105/84, 24 April 1990.

rule was that the Prime Minister had to notify the CNCIS of every wiretap authorization within 48 hours. If the CNCIS deemed the authorization illegal, it could send "recommendations" to the Prime Minister to ask for the wiretap to end (within a year, it became standard practice for the Prime Minister to wait for the CNCIS opinion before conducting wiretaps). Authorizations remained valid for four months, after which they either had to be renewed or else expire. As already noted, the Act's article 20 also granted a blank check to the DGSE to intercept wireless communications[19]

1.2 The Slow Pace of Intelligence Reform in the 2000's

Despite these past contentious episodes, however, the legal framework and overall oversight of intelligence services remained well behind "best practices" of other liberal-democratic regimes.

From the end of the 1990's on, inter- and supra-national organizations such as the Council of Europe or the European Parliament adopted a series of recommendations and resolutions laying out best-practices to ensure the democratic accountability of intelligence services.[20] These led three overarching principles:

- the Parliament should be entrusted the power authorize the creation of intelligence services;
- these agencies' interferences with fundamental rights should abide by the principle of proportionality;
- they should also be subject to both parliamentary and jurisdictional oversight.

France not only failed to comply wih these principles, but the gap kept widening. There was a sense among intelligence circles that what a former Deputy Director at the DGSE called called "a reputation once tainted by experiences of illegal surveillance of politicians, companies, and ordinary

[19] Article 20 of the Wiretapping Act provided that: "measures taken by public authorities to ensure, for the sole purpose of defending national interests, the surveillance and the control of Hertzian transmissions are not subject to title I and II of the present Act" ("*Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions des titres Ier et II de la présente loi*"). However, the CNCIS' (secret) jurisprudence allegedly forbade the use of this article to conduct, on the French territory, "the interception of communications that can be individualized and related to an identified threat." See: Jean-Pierre Raffarin. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*. Paris: Parlement français, Feb. 25, 2016. Available at: http://www.assemblee-nationale.fr/14/rap-off/i3524.asp, p. 71.

[20] Sébastien-Yves Laurent. *Pour une véritable politique publique du renseignement*. Paris: Institut Montaigne, 2014, p. 96. Available at: http://www.institutmontaigne.org/fr/publications/pour-une-veritable-politique-publique-du-renseignement, p. 37.

citizens" deserved to be improved.[21] That meant engaging in both reorganization and partial legalization.

Governance reforms

In the second half of the 2000's, policymakers made a timid but sustained effort to streamline oversight and chains of command.

- In the Fall of 2007, the Sarkozy government introduced a bill establishing the "parliamentary Delegation for Intelligence" (*Délégation parlementaire au renseignement*, or DPR), an eight-member strong bipartisan parliamentary committee charged with "keeping track (*suivi*) of the general activity and means" of intelligence agencies.[22] This was a tepid move, but nevertheless amounted to significant change: For the first time, the executive branch conceded to the legislative branch –which is structurally weak under the political regime of the Fifth Republic– some degree of first-hand knowledge of what was until then a *chasse gardée*.[23]

- Inspired by the U.S. style of intelligence governance, several reforms also aimed at strengthening the "*présidentialisation*" of intelligence policy. In 2008, the Élysée created the office of National Intelligence Coordinator as well as the National Intelligence Council. At least on paper (because the President already had *de facto* authority on the DGSE), the reform undermined the Prime Minister's authority over intelligence agencies.

- Another major reform was enacted in 2008 to reorganize domestic intelligence. A decree merged the central Directorate of the *Renseignements généraux* (RG) with the *Direction de la Surveillance du territoire* (DST) (in charge of counterespionage and counterterrorism). In 2012, domestic intelligence services took the name of *Direction générale de la Sécurité Intérieure* (DGSI), and were placed under the direct authority of the Minister of the Interior.[24]

- In May 2011, two executive orders (*arrêtés*) officially recognized six agencies as part of the national "intelligence community."[25]

[21] Philippe Hayez. ""Renseignement": The New French Intelligence Policy". *International Journal of Intelligence and CounterIntelligence* 23.3 (June 8, 2010), pp. 474–486, p. 474.

[22] *Loi n° 2007-1443 du 9 octobre 2007*.

[23] It was not until 2013, however, that the law was amended to substitute the word "*contrôle*" to that of "*suivi*," thereby recognizing the delegation's oversight function.

[24] *Décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure*.

[25] *Arrêté du 9 mai 2011 pris en application du troisième alinéa du I de l'article L. 2371-*

- Finally, in July 2014, an *Inspection générale des services de renseignement* was created under the authority of the Prime Minister (in partnership with the National Intelligence Coordinator) to audit intelligence agencies and advise political authorities.[26]

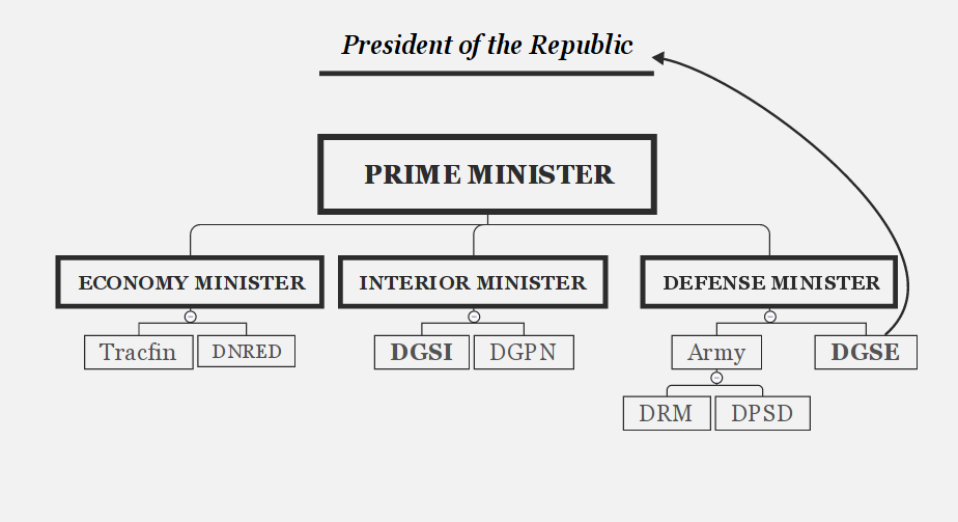

Figure 3: Organigram of the French intelligence community.

Of course, these incremental changes did little to compensate for the growing gap between the law and the surveillance capabilities of intelligence agencies.

Access to metadata

By the early 2000's, Internet traffic was becoming ubiquitous, as much of the world's communications moved to IP networks. To control what many saw as a "lawless" cyberspace, many groups both in and out of government felt that legal reforms were needed to facilitate both law enforcement and intelligence.

In August 2000, as it was passing a major reform of the audiovisual sector, the French Parliament took on to establish *ad hoc* legal foundations to regulate Internet communications.[27] In particular, the law's article 43-9 mandated hosting providers to retain "data allowing the identification of

1 du code de la défense and *arrêté du 9 mai 2014 portant application de la réforme des services de renseignement du ministère de l'intérieur.*

[26] *Décret n° 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement.*

[27] *Loi 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.*

anybody who contributed to the creation of content" on their online services.[28]

Suddenly, the 9/11 attacks provided security professionals and their political allies with new-found justifications to extend the reach of Internet surveillance, under the guise of "politics of exception" that (anti)terrorism mandated.[29] Following the attacks, as the US Congress passed the PATRIOT Act, both French and British parliaments amended their national law to force telecom operators to retain their users' telephone and Internet metadata.[30]

At this point in time, French law only allowed civil and criminal courts to access retained data,[31] and –like in the UK– data retention was introduced as a "sunset," two-year long provision justified by an imperious terrorist threat. In March 2006 however, the provision was made permanent through a new vote in Parliament,[32] though it was only in March 2006 that its implementation decree was adopted.[33]

Also in 2006, the Madrid and London attacks prompted EU lawmakers to extend mandatory data retention to all of Member States through the ill-fated 2006 data retention directive (eventually struck down by the Court of Justice of the European Union in 2014).[34] In France, despite criticisms from the government's own human rights watchdog,[35] French intelligence services were finally given a legislative mandate to access two categories of data,[36] though only for the purpose of preventing terrorist attacks:

[28]The provision was later moved to article 6-II of an Internet-specific law adopted in 2004 to implement the 2000 eCommerce directive, the *loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*.

[29]Didier Bigo and Anastassia Tsoukala, eds. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. 1 edition. London; New York: Routledge, 2008. 208 pp.

[30]In the UK, the Parliament adopted the Anti-Terrorism, Crime and Security (ATCS) Act in November 2001, whereas France passed article 29 of *loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne* (LSQ).

[31]Note that in France, uncertainties about the actual scope of the categories of data falling under this regime remain to this day (Marc Rees. *Loi Renseignement : l'avis que la CNIL refuse de publier*. Feb. 10, 2016. Available at: http://www.nextinpact.com/news/98483-loi-renseignement-avis-que-cnil-refuse-publier.htm).

[32]*Loi n° 2003-1062 du 15 novembre 2001 relative à la sécurité quotidienne* (LSQ).

[33]*Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques*.

[34]CJUE, *Digital Rights Ireland v. Ireland*, C-293/12 , April 14 2014.

[35]Commenting on the Bill, the *Commission nationale consultative des droits de l'Homme* wrote the following: "*Une fois encore, au développement des pouvoirs de police administrative dans la mise en place de ce système de surveillance d'une activité privée des citoyens dans des lieux d'expression publics que sont les cybercafés, le tout au détriment des prérogatives auparavant laissées à la seule autorité judiciaire gardienne des libertés. C'est d'abord cette dérive qui est inquiétante*". (*Projet de loi relatif à la sécurité et à la lutte contre le terrorisme - Analyse*. Ligue des droits de l'Homme, Oct. 5, 2012. Available at: http://www.ldh-france.org/IMG/pdf/analyse_du_projet_de_loi.pdf).

[36]See article 6 of the *loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le ter-*

- the metadata retained by telecom operators, whose scope was defined for the first time in the decree of March 2006 as including "data allowing user identification," "data related to the terminal equipments used," "the technical features as well as the date, time and duration of every communication" and "data allowing the identification of the communication recipient(s)."[37]

- identifying data held by hosting providers for the users of online service who "contributed content." The precise scope of this category would not be defined until the adoption of a decree in 2011. It includes, among other things, IP addresses, date and time of the connexion, pseudonyms and, where relevant for hosting providers specifically, account information such as pseudonyms, email addresses and passwords.[38]

At the time, this administrative access to Internet metadata was justified by securitization discourses pointing to the danger of cybercafes and open Wifi networks, which the government argued allowed for anonymous communications.[39] During the debate, the Bill's proponents recalled that 9/11 attackers had used cybercafes to cover their tracks.

Also introduced as a sunset provision, administrative metadata access was prolonged a first time in December 2008 and then again in December 2012, despite criticisms from the French Human Rights League.[40]

Internet wiretaps

As for Internet wiretaps –that is not only access to the metadata but also the content of Internet communications ("(*correspondances*" in French)–, we have already seen how the foreign intelligence agency, the DGSE, was allowed to go roll-out a program of large-scale surveillance of fiber-optic cables going in and out of France.

Before Vincent Jauvert's article of July 2015, officials from the DGSE had already hinted at the formidable growth of its Internet surveillance capabilities. In 2010, the Chief Technology Officer of the agency, Bernard Barbier, who was then supervising the plan agreed upon in Sarkozy's office two

rorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

[37]See the definition provided in article 1 of the 2006 decree. Note that the retention period of the metadata collected by intelligence agencies would not be specified until the LPM decree of 2014, which set a data retention period of 3 years.

[38]See article 1 of the *décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* .

[39]See the Bill's explanatory memorandum, available at https://archive.is/jlcj4.

[40]See *loi n°2008-1245 du 1er décembre 2008* and *loi n°2012-1432 du 21 décembre 2012*. For the comments of the Human Rights League's on the 2012 law, see: *Projet de loi relatif à la sécurité et à la lutte contre le terrorisme - Analyse*, p. 2.

years earlier, boasted during a public talk before the Cryptographers' Reserve that France was in the "first division" of communications intelligence. He revealed for what was probably the first time that public networks were now the DGSE's "main target."[41] In March 2013, just a few weeks before the beginning of the Snowden disclosures, the head of the DGSE was even less equivocal, admitting before the National Assembly that, since 2008, "we have been able to develop a significant plan for the surveillance of Internet traffic."[42]

Of course, these new surveillance programs were outside of any sound legal framework. The sitting Director of the DGSE, Bertrand Bajolet, would later explain that the oversight commission, the CNCIS, had developed what he called a "creative case law" to accommodate these new-found capabilities[43]

As we saw, news reports suggest that among these *ad hoc* rules, the CNCIS was able to conduct some degree oversight, but only on broad authorizations: Though they had to fall in the field of competence of intelligence agencies (e.g. fight against terrorism, nuclear proliferation, economic intelligence), these surveillance authorizations did not have to target specific individuals, and instead allowed for the collection of huge swaths of communications coming from a given country. Second, any communication between two French residents collected in transit had to be automatically rejected from the system. And third, the DGSE was not allowed to spy on other EU countries such as Germany –this is quite ironic considering the 2015 revelations pointing to the surveillance of France by the German BND, *on behalf* of the NSA.[44]

Of course, these rules were secret, and it is therefore impossible to verify the veracity of these claims, nor if they were respected by the DGSE. But recent revelations of a spying case against a local political opponent of one of Sarkozy's closest allies suggests they could easily be circumvented through what insiders euphemistically called an "alegal casuistic." For instance, some in the agency apparently contended that such domestic and political surveil-

[41] Quoted in: Jean Marc Manach. *Frenchelon: la DGSE est en « 1ère division »*. BUG BROTHER. Oct. 2, 2010. Available at: http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division/.

[42] *Audition du préfet Érard Corbin de Mangoux, Directeur général de la sécurité extérieure (DGSE) au ministère de la Défense.* Compte rendu n°56. Paris: Assemblée nationale, commission de la défense nationale et des forces armées, Feb. 20, 2013. Available at: http://www.assemblee-nationale.fr/14/cr-cdef/12-13/c1213056.asp.

[43] *Audition de M. Bernard Bajolet, directeur général de la sécurité extérieure, sur le projet de loi relatif au renseignement.* Compte rendu de séance n°47. Paris: Assemblée nationale, commission de la défense nationale et des forces armées, Mar. 24, 2015. Available at: http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415047.asp#P3_69.

[44] Maik Baumgärtner et al. *Spying Close to Home: German Intelligence Under Fire for NSA Cooperation.* Apr. 24, 2015. Available at: http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html.

lance was perfectly legal under the Hertzian provision included in the 1991 Wiretapping Act.[45]

As for surveillance conducted by domestic intelligence agencies, the Wiretapping Act was also quietly amended in 2004 by the government through a law adopted to transpose EU directives in the field of telecommunications.[46] This legislative patch changed the word "telecommunications" for "electronic communications," which was deemed enough to extend the Act's scope to Internet communications.[47]

As we will see, this should have raised eyebrows. In 1991, lawmakers made the law with the wired telephone in mind, not for the Internet. Considering that the latter represents a much broader category of communications than telephone calls, including both public and private communications, a new legislation should have been necessary to comply with the ECHR's test.

Secret interpretations of intelligence laws constitute a common trait across the transnational intelligence field. Still, the case of France contrasts with the approach of some of its closest allies and competitors, and in particular that of the United Kingdom. As early as 2000, Prime Minister Tony Blair had chosen a rather "ambitious" route to regulate Internet surveillance with the adoption of the Regulation of Investigatory Powers Act (RIPA), explicitly framed as a way of adapting the legal framework underlying communications surveillance to the Internet.[48] In France, on the contrary, the extension of the legal regime to cover online surveillance was done without any notice, with only *ex post* and indirect confirmations that both foreign and domestic intelligence agencies were *de facto* tapping into

[45] Jacques Follorou. *Comment la DGSE a pu espionner des Français*. May 2016. Available at: http://www.lemonde.fr/societe/article/2016/04/13/comment-la-dgse-a-pu-espionner-des-francais_4901155_3224.html; Jacques Follorou. *Comment la DGSE a surveillé Thierry Solère*. Apr. 12, 2016. Available at: http://www.lemonde.fr/societe/article/2016/04/12/comment-la-dgse-a-surveille-thierry-solere_4900451_3224.html.

[46] *Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle*.

[47] The domestic wiretap provision was interpreted as covering Internet communications. But the hertzian provision of 1991 also seem to have been used to bypass the *ex ante* oversight of the CNCIS. This is at any rate the argument used by the former head of the DCRI, Bernad Squarcini, to justify his request of a reporter's telephone records in the course of a secret investigation on an leak that embarrassed the Sarkozy government in 2010. Squarcini eventually lost the case in 2014, when a Paris court ruled that such surveillance could not be used for the targeted surveillance of an individual (see footnote 19). He was sentenced to a €8000 fine. See: *Affaire des fadettes : Squarcini condamné à 8000 euros d'amende*. Mediapart. Apr. 8, 2014. Available at: https://www.mediapart.fr/journal/france/080414/affaire-des-fadettes-squarcini-condamne-8000-euros-damende.

[48] In fact, here too it was legalization of existing "alegal" practices: Large-scale Internet surveillance had already been conducted prior to 2000 under section 94 of the Telecommunication Act of 1984. See: Owen Bowcott and Richard Norton-Taylor. *UK spy agencies have collected bulk personal data since 1990s, files show*. Apr. 21, 2016. Available at: http://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s.

Internet communications.[49]

1.3 Justifications for Legalization

The French legal framework was thus severely lacking, pushing deep state officials to develop secret interpretations stretching the scope of existing provisions to cover new surveillance capabilities. Eventually, these needed to be secured at the legislative level.

In July 2008, the government released a White Paper of Defense and National Security –a major effort of strategic planning conducted under Sarkozy's presidency. For what appears to be the first time, this official policy document claimed that intelligence legislation would soon be presented to Parliament:

> Intelligence activities do not have the benefit of a clear and sufficient legal framework. This shortcoming must be corrected. A new legal architecture will define the duties of intelligence agencies, safeguards for both their personnels and human sources, as well as the main arrangements for the protection of classified information. Legislative adjustments will be provided, while respecting the balance between the protection of civil rights, the effectiveness of judicial proceedings and the protection of secrecy (...).[50]

Referring to the administrative access to metadata, the White Paper added that "the consultation of metadata and administrative databases (...) will be enlarged."

But the following September, a major scandal erupted around the adoption of a decree authorizing a very broad intelligence database –named EDVIGE– for domestic surveillance purposes. In a few weeks time, widespread civil society opposition against the decree led the government to backtrack.[51]

[49] For instance, referring to the "Interdepartmental Oversight Group" (*Groupement interministériel de contrôle*, or GIC) –the body which under the authority of the Prime Minister is in charge of centralizing the technical operations related to administrative wiretaps–, the CNCIS 2015 annual report stressed that: "The GIC has to permanently adapt to technological advances in the field of electronic communications, which always leads to formidable challenges to overcome. It had to integrate, since 1991, wireless telephony, SMS, MMS, the Internet (...)" (*22e rapport d'activité 2013-2014*. Paris: CNCIS, 2015. Available at: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101/0000.pdf, p. 88).

[50] *Livre blanc sur la Défense et la Sécurité nationale*. Paris: Gouvernement français, June 2008, p. 142.

[51] For an overview of the civil society contention against the "EDVIGE file," see: Meryem Marzouki. "« Non à Edvige » : sursaut ou prise de conscience ?" *Plein droit* 80 (Mar. 1, 2009), pp. 21–26. Available at: http://www.cairn.info/resume.php?ID_ARTICLE=PLD_080_0021.

The mobilization marked one of the biggest episode of human right contention under Sarkozy's presidency and it was apparently enough to put the government's broader plans for modernizing intelligence law to rest until the end of its mandate.

Ironically, what a conservative, "tough on security" government could not achieve for political reasons would eventually be done by left-wing, supposedly pro-civil rights Party.

Indeed, in 2011, with the general election fast approaching, representatives from the Socialist Party seized the opportunity. At first in opposition, their calls for legalization took the form of a political commitment to make intelligence policy an acknowledged public policy, in line with international standards. Once Socialists got back to power, they would turn into a more detailed plan to expand the legal basis for the COMINT activities of French intelligence services so as to secure the work of people in the intelligence community, paving the way for the major intelligence reform enacted in 2015.

Two men played a key role in this process.

The first is Jean-Jacques Urvoas. In less than a decade, he went from the status of a virtually unknown lecturer in law and local socialist apparatchik to that of Minister of Justice. He first joined the benches of the National Assembly in 2007. At the time, he was a local official coming from Brest, in Brittany, but he quickly rose within the Socialist Party and became the National Secretary for Security Affairs in 2009. A year later, he was appointed to CNCIS as the representative of the parliamentary opposition. In the following months, he would often denounce the use of the domestic intelligence agency as Sarkozy's political police. In 2012, when the Socialist Party won both the presidential and the legislative elections, Urvoas was re-elected to the National Assembly and awarded with the prestigious position of President of the committee on Legal Affairs. This also made him a *de facto* member of the Parliament's Committee on Intelligence, the DPR, sealing his membership to the small circle of intelligence policy-makers.

The second important character is Floran Vadillo. Born in 1985, he quickly became Urvoas' closest adviser on intelligence reform. In 2012, after a Masters thesis on the history of the Socialist Party's relationship with intelligence agencies, Vadillo completed a PhD thesis on the role of the Élysée in anti-terrorist policies under the Fifth Republic. During the course of this research, Vadillo had become acquainted with powerful officials within intelligence community, to such an extent that, according to investigative journalists, it is thanks to Bernard Squarcini –the former head of the domestic intelligence agency– that Vadillo met with Urvoas in 2011.[52]

Though still young, Vadillo came not only with a strong connections in

[52]Didier Hassoux, Christophe Labbe, and Olivia Recasens. *L'espion du président*. Paris: Robert Laffont, 2012. 193 pp.

the intelligence world but also with good knowledge of the Socialist Party politics and its equivocal relationship to intelligence services. In the run-up to the 2012 election, he would help Urvoas forge the Party's doctrine on these issues, as the two men sought to use reconcile intelligence practices with the law and good politics. To do so, they publicly relayed calls for legalization coming from both legal scholars and intelligence practitioners, aiming to shape an upcoming intelligence reform.

In April 2011, the pair published a first report for the Jean-Jaurès Foundation (a think tank affiliated with the Socialist Party).[53] Entitled "Reforming Intelligence Services," the report offered to reconcile the deep state and its exceptional powers with democracy and the rule of law. In this document, Urvoas and Vadillo mocked the 1971 political platform of François Mitterrand's Socialist Party for exhibiting strong resentment against intelligence services –at the time, the French Left had promised to crack down on their power and even to abolish the SDECE (the predecessor of the DGSE). Urvoas and Vadillo's message, aimed at security professionals in particular, was clear: These naïve times were over, and the Party now had serious proposals to put forward.

Pointing to the shortcomings of the current legal framework compared to other European countries, they claimed that "arguments of opportunity and expediency as well as the democratic logic plead[ed] in favor of an action that would correct this deficiency." To do so, they formulated thirty-six proposals. One, for instance, offered to inscribe intelligence services in a proper legislative framework. Others aimed to decrease the "presidentialization" of intelligence governance and instead reinforce the power of both the Prime Minister and the Parliament. The authors also stressed the legal risks of inaction for intelligence agencies:

> The patchwork of texts presiding over their activity is obviously not sufficient to protect France from a condemnation by the European Court of Human Rights.

Then, a year later, just before the presidential election, Vadillo published another brief for the same think tank.[54] Following a similar political line as the paper co-authored with Urvoas, it nevertheless brought new details on what intelligence reform should look like, prefiguring what would become the Intelligence Act of 2015. Among other things, the brief argued that

[53] Jean-Jacques Urvoas and Floran Vadillo. *Réformer les services de renseignement français*. Paris: Fondation Jean Jaurès, May 2, 2011, p. 44. Available at: http://www.jean-jaures.org/Publications/Essais/Reformer-les-services-de-renseignement-francais.

[54] Floran Vadillo. *Une loi relative aux services de renseignement : l'utopie d'une démocratie adulte ?* Paris: Fondation Jean Jaurès, Apr. 18, 2012. Available at: http://www.jean-jaures.org/Publications/Notes/Une-loi-relative-aux-services-de-renseignement-l-utopie-d-une-democratie-adulte.

such a law would have to precisely lay out the missions of intelligence agencies, clarify the exact scope of the intelligence community and create legal definitions for intelligence-gathering techniques. It reiterated calls for the creation of an administrative but independent oversight commission to replace the CNCIS and conduct *ex ante* review of surveillance authorizations, but also audit the use of "special funds" going to intelligence agencies.

The elections of May and June 2012 saw the Socialist Party seize both the Presidency and the Parliament. In August, after had Urvoas reached the presidency of the committee on Legal Affairs at the National Assembly, Vadillo officially joined his staff.

Then, mid-May 2013 –just two weeks before the first Guardian article based on the Snowden files–, the committee adopted a 200-page long report on the "evolution of the legal framework of intelligence services."[55] Though issued in the name of a special study committee of fifteen *députés* from both sides of the aisle, the report represented a unique opportunity for the Urvoas-Vadillo duo to push their research and proposals in more formal policy settings. These were also enriched by discussions held with members of the intelligence community during the hearings carried on by the committee.

In this important report, justification discourses appeared somewhat more refined. The document stressed that, both in terms of budget and staff, French agencies were less resourced that their Western counterparts, and that adapting the legal framework would allow them to be more effective in the fight against terrorism and organized crime. It also reviewed the new surveillance capabilities that had been authorized for judicial investigations in the past years, such as computer network exploitation (e.g. hacking).[56] The report clearly admitted that such practices were already carried on, relaying the notion apparently borrowed to intelligence officials of "alegality" (*a-légalité*), and went at length to stress the need secure them legally:

> The time is over when the state and its administrations could escape administrative, national or even international courts, or the media's acuteness. The features of our democratic system now imply the existence of powerful counter-powers that threaten intelligence agencies because of the precariousness of the legal framework in these these agencies operate.[57]

[55] Jean-Jacques Urvoas and Patrice Verchère. *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement.* Commission des Lois 1022. Paris: Assemblée nationale, May 14, 2013. Available at: http://www.assemblee-nationale.fr/14/controle/lois/renseignement.asp.

[56] Computer network exploitation (CNE) is a technique through which computer networks are used to infiltrate target computers' networks in order to extract and gather intelligence data. In sum, it refers to computer intrusion, or "hacking," carried on for intelligence purposes. It was authorized in France in 2011 for judicial investigations.

[57] Urvoas and Verchère, *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, p. 29.

In one section titled "Tomorrow, a condemnation by the ECHR?," the report provided a overview of the Court's case law and insisted that:

> In France, for lack of legislation adapted to certain aspects of their activities, intelligence services are forced to act outside of any legal framework. Indeed, national security and the anti-terrorist fight can justify the implementation of special investigation techniques, the use of which is not yet authorized by law outside of the judicial framework. Now, the techniques being used amount, by nature and by necessity, to interferences with rights and freedoms. The interception of communication, the listening of places and the tapping of images violate the right to private life, as do the geo-localization of a phone or of a vehicle.
>
> Even if these techniques are legitimately implemented, it is totally anomalous, in a state abiding by the rule of law, for interferences with rights and freedoms to occur outside of any legal framework. Concretely, France is risking a condemnation by the European Court of Human Rights for violating the European Convention on Human Rights. For the time being, no legal challenge has been introduced against intelligence-related activities, but there is a constant risk of condemnation.[58]

Recalling the 1990 rulings against France on the same topic, the section ended with an invitation to engage in an intelligence reform based on a careful analysis of the ECHR case law in the field of secret surveillance. But despite this acknowledgement that intelligence agencies had been engaging in illegal surveillance, no human right group picked up on it.

2 After Snowden, Legalization Sparked Contention

At the outset of the Snowden disclosures, France's legal patch-ups for both domestic and, even more so, for foreign intelligence made the main actors of COMINT policy strongly insecure. But while the global anti-surveillance contention unleashed by Snowden reinforced the need for legalization, it also made it more politically risky. In late-2013, an attempt at partial legalization gave rise to new coordination within civil society groups opposed to large-scale surveillance, and reinforced these fears. It was only with the spectacular rise of the Islamic State in 2014 and the Paris attacks of January 2015 that new securitization discourses created the political conditions for the passage of the long-awaited Intelligence Act.

[58] Urvoas and Verchère, *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, p. 31.

2.1 Initial (Lack of) Contention

It is useful to start by noting that the French civil society reaction to the Snowden disclosure –the first of which appeared in Guardian article on June 5th, 2013– was relatively mild.

Like in the US, the UK, Germany, and other countries, there was of course widespread media coverage of the Snowden affair in June, July and August of that year (see figure 4). Many French Non-Governmental Organizations (NGOs) active in the field of digital rights or wide human rights joined the media frenzy, supplying analysis through appearances and TV studios and various Op-Eds. But apart from this, there was little contention coming from French human rights activists.

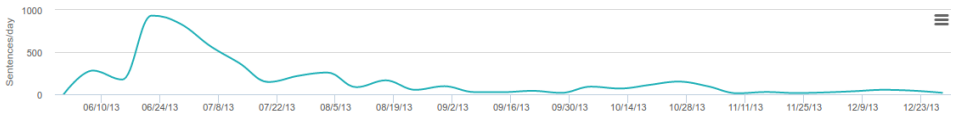

Figure 4: Number of sentences per day mentioning the term "Snowden" in national online news sources in France (based on 129 media sources) from June 2013 to January 2014 (MediaMeter).

Some international organizations with presence in France, like Amnesty or Human Rights Watch, were able to get traction from the initiatives launched elsewhere, occupying the French public sphere by translating press releases. French digital rights organizations working on data protection reform, like *La Quadrature du Net* (LQDN), mentioned Snowden in passing in their public communications on the matter, but were focusing on the data collection practices of Internet firms rather than state surveillance.

The only notable exception to this relative apathy was the FIDH, the worldwide movement for human rights, founded in 1922 in France and headquarted in Paris.[59] On July 11th, working with a Parisian law firm specialized in human rights, the FIDH filed a criminal complaint against NSA's PRISM program.[60] The next day, the organization announced that it had

[59]The "FIDH exception" can perhaps be accounted for by the fact that prior to the Snowden disclosures, in 2011 and 2012, the organization had initiated legal challenges (some of them in partnership with the Human Rights League) against the French companies Amesys and Qosmos for supplying the Libyan and Syrian regimes with top-notch Internet surveillance capabilities. See: Jérôme Hourdeaux. *Surveillance: la justice enquête sur les liens entre Qosmos et la Syrie*. Mediapart. Apr. 11, 2014. Available at: https://www.mediapart.fr/journal/international/110414/surveillance-la-justice-enquete-sur-les-liens-entre-qosmos-et-la-syrie; Jérôme Hourdeaux, Bluetouff, and Kitetoa. *Qosmos : du projet universitaire aux activités "secret-défense"*. Mediapart. May 7, 2014. Available at: https://www.mediapart.fr/journal/international/070514/qosmos-du-projet-universitaire-aux-activites-secret-defense; *The Amesys Case*. Paris: FIDH, Feb. 11, 2015. Available at: https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf.

[60]PRISM is a US clandestine surveillance program launched in 2007 under which the

appealed to the U.N. Special Rapporteur for Freedom of Expression, Frank La Rue, calling for an investigation into the facts revealed by Snowden (quite presciently, La Rue's 2013 annual report, released in April of that year, focused on the interplay between freedom of expression and communications surveillance).[61]

Silence and distinction strategies

How can we explain such lack of substantive mobilization in France in the immediate aftermath of the Snowden revelations? For one thing, even in activist circles, there was a feeling that the whole affair was mostly related to the NSA and the GCHQ, not French agencies. When on June 12$^{\text{th}}$, Urvoas was interviewed in *Le Monde*, he denied that French agencies were conducting large-scale surveillance of Internet communications, claiming:

> During the investigation I conducted for the parliamentary report [on the evolution of the legal framework of intelligence agencies], I have not encountered any similar surveillance program in France. I have never heard of tools that could be associated to what the Americans use, and every time I asked intelligence officials, I got a negative answer.[62]

At the time, Guardian articles had only mentioned PRISM, the NSA hacking capabilities, its Boundless Informant program,[63] but not the programs most akin to the DGSE large-scale surveillance techniques, that is to say the NSA's Upstream collection program or the GCHQ's Tempora program.[64] So, even though as a member of the CNCIS he was very likely

United States National Security Agency (NSA) collects internet communications from at least nine major US Internet companies (source: Wikipedia).

[61] Frank La Rue. *2013 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Geneva: United Nations Human Rights Council, Apr. 2013. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[62] Nicolas Chapuis. *Urvoas : "Je n'ai pas rencontré de programme de surveillance similaire en France"*. June 12, 2013. Available at: http://www.lemonde.fr/politique/article/2013/06/12/urvoas-je-n-ai-pas-rencontre-de-programme-de-surveillance-similaire-en-france_3428507_823448.html.

[63] Boundless Informant is a big data analysis and data visualization tool used by the NSA. It gives NSA managers summaries of the NSA's worldwide data collection activities by counting metadata (source: Wikipedia).

[64] Upstream collection is a term used by the NSA for intercepting telephone and Internet traffic from the internet backbone, i.e. major internet cables and switches, both domestic and foreign. It is comprised of four distinct major surveillance program codenamed FAIRVIEW, BLARNEY, STORMBREW and OAKSTAR. Parts of these programs had been unveiled by whistleblower Mark Klein as early as 2006 (source: Wikipedia).

TEMPORA is the codeword for a formerly secret computer system that is used by the British GCHQ. This system is used to buffer most Internet communications that

aware of the DGSE's large-scale surveillance capabilities, including its reliance on computer hacking, Urvoas may have been playing on words but his statement was not totally incorrect.

Then, two weeks later, on July 4th *Le Monde* ran a piece by reporter Jacques Follorou on the "French Big Brother," claiming that France was "doing the same thing" as the NSA:

> *Le Monde* is able to reveal the General-Directorate for External Security (DGSE, special services) systematically collects electromagnetic signals coming from computers or telephones in France, as well as traffic between French and foreigners: the totality of our communications are being spied upon. All emails, SMS, telephone records, connections to Facebook, Twitter, is then stored for years.[65]

The report further claimed the DGSE's technical Directorate was sharing 80 % of its surveillance tools with domestic agencies, acting as a *de facto* "fusion center." It also quoted a high-ranking intelligence officials arguing that these practices were "alegal" rather than illegal.

Considering what we now know about the DGSE's Internet surveillance programs and given also the provision of the 1991 wiretapping act allowing bulk collection of wireless communications,[66] the article could have triggered a new scandal. But because of its sensationalist tone and several inaccuracies –most importantly the fact that it was technically infeasible for the DGSE to collect the "totality" of French communications–, it appeared overblown. As a consequence, it was easily dismissed.

Once again, Urvoas was at the forefront of this distinction strategy. He immediately published a blog post refuting these allegations. "No," Urvoas argued, "French citizens are not subject to a massive and permanent spying outside of any oversight." Again, every word of the sentence was carefully chosen to make the statement truthful and deny that suspicionless, large-scale collection was also happening in France. Once more, Urvoas contrasted the DGSE's practices to that of the NSA using what would become a favored metaphor in intelligence circles:

---

are extracted from fibre-optic cables, so these can be processed and searched at a later time. Tempora uses intercepts on the fiber-optic cables that make up the backbone of the Internet to gain access to large amounts of Internet users' personal data, without any individual suspicion or targeting. The intercepts are placed in the United Kingdom and overseas, with the knowledge of companies owning either the cables or landing stations (source: Wikipedia).

[65] Jacques Follorou and Franck Johannès. *La totalité de nos communications espionnées par un supercalculateur*. July 4, 2013. Available at: http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.

[66] See footnote 19.

> To the difference of the NSA, a technical agency dedicated only to interceptions, the DGSE is a non-specialized agency collecting intelligence in the sole purpose of complying with its regulatory duties. We could thus say that, against the 'fishing trawls' that the NSA seems to be operating, the DGSE is conducting 'harpoon fishing' as part of its prerogatives.[67]

But the dismissal of *Le Monde*'s account did not only came from policy-makers. Jean-March Manach, a journalist, surveillance expert and privacy advocate, also bemoaned *Le Monde*'s journalists paranoid tone.[68] Manach also stressed that many of *Le Monde*'s claims, which quoted some of his own articles on the so-called "Frenchelon" DGSE surveillance program, were in fact not new and had been documented before.

Advocacy failure

Manach was right, which in turn begs the question of why, in the immediate aftermath of the Snowden disclosures and even both *prior* to that, it took so long for human rights groups in France to pick up on the pieces of information already available and go after these illegal surveillance operations, both in courts and in policy-making arenas.

The question is a complex one, and cannot be fully addressed here. But two aspects deserve to be mentioned. First, regarding strategic litigation, it is worth noting that in the French legal system, legal opportunities had been lacking. Statements by officials –like those by the heads of DGSE is 2010 and 2013– are not enough to initiate legal action. In other countries like the US, they might help trigger successful "FOIA requests" (named after the 1966 Freedom of Information Act). In France however, the national "freedom of information" law adopted in 1978 has extremely broad national security exemptions and is generally much weaker (for instance, the request must specify the exact name of the documents sought after, which represents a formidable hurdle in policy areas covered by state secrets).

Second, and more importantly, the lack of mobilization prior and in the immediate aftermath of the first Snowden disclosures speaks about the weaknesses of online privacy advocacy in France, at least until late-2013. Even when in October 2013, thanks to the Snowden trove, the existence of the so-called LUSTRE data-sharing agreement between the NSA and the DGSE was revealed by *Le Monde*, showing that the latter shared millions of metadata records everyday with the US agency some of them very likely

[67] Jean-Jacques Urvoas. *Big Brother à la française ? Commentaires.* Le blog de Jean-Jacques Urvoas. July 4, 2013. Available at: http://archive.is/7SGgk.

[68] Jean-Marc Manach. *La DGSE a le « droit » d'espionner ton Wi-Fi, ton GSM et ton GPS aussi.* BUG BROTHER. July 11, 2013. Available at: http://www.lemonde.fr/iframe/jelec.html.

related to French citizens, human rights advocacy group did not pick up on the issue.

Though there have recent and successful episodes of contention about offline surveillance and intelligence files,[69] Internet surveillance has remained out of the focus of larger human rights organizations and small digital rights groups, whose expertise on the issue has for the most part remained fragile. On the contrary, US, British, German or Brazilian groups working on the issue appear much more resourced. Historical factors, past legalization processes and leaks on Internet surveillance programs have allowed them maintain stronger networks and build expertise.

One major moment of the transnational post-Snowden contention, for instance, was the release of the "International Principles on the Application of Human Rights to Communications Surveillance" in May 2014. Framed as a key global response of civil society to the Snowden controversies, the work on this text started as early as 2012, as noted in the document:

> More than 40 privacy and security experts participated in the drafting process through the Brussels meeting organized by Privacy International in October 2012, the Brazil meeting organized by EFF in December 2012 as well as all those experts who submitted comments via the online consultation.

French activists seem to have remained largely outside of these transnational networks working on state surveillance. It was only when post-Snowden legalization efforts started to materialize that they eventually built capacity to fight against illegitimate forms of state surveillance.

2.2 A Trial Baloon for Legalization: The 2013 Military Planning Act

These structural weaknesses of anti-surveillance advocacy in France help explain why civil society groups failed to react in time to the first legalization attempt, which occurred in October 2013.

Legalizing "alegal" access to metadata

Urvoas' May 2013 report stressed the importance of metadata for intelligence work. It also claimed –less convincingly– that "the requisition of [metadata] is a much less intrusive process for privacy than the practice of telephone wiretapping."[70] But most importantly, it revealed that according to legal

[69] See for instance contention against the "EDVIGE file" in 2008: Marzouki, "« Non à Edvige »".

[70] Urvoas and Verchère, *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, p. 23. Such a claim would be contradicted, *inter alia*, by the ECJ *Digital Rights* ruling (see 34.

casuistic developed in deep state circles, there were actually two means for intelligence services to access telephone and Internet metadata:

- One was the well-known procedure opened by the 2006 Terrorism Act, allowing access to metadata retained by telecom operators and hosting providers, only for anti-terrorism purposes (about 30,000 requests a year in 2012). The *ex ante* oversight was conducted by a person designated by the CNCIS, and the later was charged with the *ex post* control.

- The other one, much less known, was opened by article L. 244-2 of the Code of Internal Security, created by the 1991 Wiretapping Law. It allowed intelligence services to request metadata to make preparations for an interception, this time for *any purpose* falling under their attributions and with no independent oversight (197,000 requests a year).

Therefore, quite against the spirit of both the 1991 and 2006 laws, intelligence services had been using a workaround to expand their access to metadata for surveillance purposes. From 2009 on, they apparently apparently experimented with the traffic-scanning devices provided by Qosmos and installed on the infrastructure of major telecom operators to do so.[71]

Though politicians had remained quite discreet about the use of this second legal regime, this information was not secret. As a matter of fact, as early as November 2012, as the Parliament was wrapping up its work on another law dealing with terrorism, Manuel Valls, then Interior Minister, declared in plenary session that the two legal regimes needed to be "reunited," and that "the Parliament would be closely associated" to the legal maneuver.[72] The Urvoas report only reiterated these calls. As already mentioned, it also stressed that certain types of surveillance actitity, such as geotagging, were conducted outside of any legal framework, and called for allowing real-time geotagging.

All this to say: Though virtually no one in the advocacy sphere took notice, there were clear signs that the government was going to legislate on the matter. As a matter of fact, this first attempt at partial legalization was quietly introduced a few weeks later. In August 2013, Manuel Valls

[71] Jérôme Hourdeaux. *Comment les services de renseignement ont mis en place une surveillance générale du Net dès 2009.* Mediapart. June 6, 2016. Available at: https://www.mediapart.fr/journal/france/060616/comment-les-services-de-renseignement-ont-mis-en-place-une-surveillance-generale-du-net-des-2009; Reflets.info. *Qosmos et le gouvernement Français, très à l'écoute du Net dès 2009.* Reflets. June 6, 2016. Available at: https://reflets.info/qosmos-et-le-gouvernement-francais-tres-a-lecoute-du-net-des-2009/.

[72] Urvoas and Verchère, *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, p. 24.

presented the 2014-2019 Military Planning Bill (*Loi de programmation militaire* or LPM), whose article 13 sought to legalize these existing "alegal" practices. First presented as a way too boost intelligence capabilities in the fight against terrorism while bringing news safeguards, the government's proposal provided intelligence agencies with both ex post and real-time access to metadata, including geographic metadata. Quite shockingly, it did not come with any oversight mechanism.

For socialist Jean-Pierre Sueur, head of the Senate's Legal Affairs committee, article 13 seemed at once too far-fetched (for lack of oversight) and too narrow (for covering only terrorism). More in line with the Urvoas report, Sueur tabled an amendment which, so to speak, aimed at keeping "the best of both worlds." It enlarged the scope of the 2006 metadata access regime to the whole spectrum of intelligence policy goals, not just terrorism, while keeping the oversight mechanism provided for in that law. It also explicitly threw geotagging data in the mix and, finally, carried the government's proposal to authorize real-time access to metadata (including geotagging data), subject to the same authorization procedure but for a duration of ten days (rather than the usual four months).

That amendment appeared convenient to the government, who in plenary session offered a "favorable opinion" to its adoption. Compared to both existing illegal practices and the government's proposal –and though its proponents would not openly admit that, for years, intelligence services had been circumventing the 2006 law– it was easy to frame it as a progress of the rule of law.

It shouldn't have, but the amendment did come as a surprise to many in the advocacy sphere, to the extent that it even went unnoticed for quite some time.

Sequence of a partly-failed mobilization against LPM

Let us track the civil society's belated mobilization against the LPM's article 13, introduced on October 20th:

- Legal journalist Marc Rees, who covers Internet policy for the tech online media *NextInpact*, publishes an analysis of article 13 and Sueur's amendment on October 14th. No reaction by civil society, despite the fact that Rees is widely read in digital rights activist circles.

- On November 13th, after the completion of the Bill's first reading before the Senate, the National Assembly starts working on it. The media –who usually pay more attention to the legislative debate in the lower house– make a few mentions the Bill, but coverage focuses on the strategic orientations it entails for national defense and security, and it particular the Bill's spendings cuts. Article 13 goes unnoticed.

- On November 20th, the *Association des services de l'Internet communautaire* (ASIC) –a professional lobbying organization representing online social services including Google France, AOL, eBay, Facebook, Microsoft, Skype and French companies like Deezer or Dailymotion– releases a brief on article 13. The later is framed as an infringement on the right to privacy, and ASIC calls on the government and lawmakers to adopt a "moratorium" on any text creating "rules of exception" for accessing users' data. ASIC also starts a petition to relay these calls on the platform *change.org* (the later would end up only 45 "supporters"). At first, only minor online tech media relay these calls.

- Six days later, on November 26th, the prominent conservative newspaper *Le Figaro* releases a sensationalist article entitled: "Telephone, Internet: The State Will Soon Be Able to Spy on Everything." The article relays the analysis of ASIC, with quotes of the organization's head.

- Media attention on article 13 starts picking up in tech sections.

- On November 29th, ASIC and the digital economy think tank *Renaissance numérique* denounce its adoption in plenary session at the National Assembly. They frame the vote as a sign of that lawmakers' fear and ignorance towards the Internet.

- On December 3rd, the leading (though relatively small) French digital rights advocacy group, LQDN finally reacts with a press release (both in French and English) denouncing article 13: "How is it possible," it asked, "that after only a few months of Edward Snowden's revelations the French government proposes a bill so detrimental to our fundamental rights?" It is relayed by the anglophone and influential tech blog *Boing Boing*.

- The next day, on December 4th, the Minister of Digital Affairs, Fleur Pellerin, is interviewed in *Le Monde*. The interview's headline stresses that she is "the first member of the government to react on surveillance of the digital sphere.." In the interview, Pellerin introduced what would become an important justification in the coming months (both in intelligence policy debate and cybersecurity debates): Pellerin framed the Snowden disclosures –which had documented the role of Silicon Valley corporations in US surveillance programs– as a confirmation that these "hegemonic" private actors were a major threat for privacy and broader European interests, casting their defense of digital rights in France as a sign of their double-dealing on the issue.

- On December 6th, The French Digital Council –a government advisory body created in 2011 and initially focused on the digital economy – re-

leases an "Opinion on Digital Freedoms" on article 13.[73] The document deplores the lack of consultation and notes that "recent international revelations about widespread surveillance practices, facilitated by the massive collection of personal data by some platforms, have raised concerns." As a consequence, the Council decides to expand its mandate and "take up the issue of the protection of fundamental rights and freedoms profoundly changed by the digital revolution." The opinion ends on a reference to the SAFARI affair and the creation of the CNIL.

- On December 9th, as the Bill goes back to the Senate floor in second-reading, major human rights organizations join the mobilization. FIDH and the *Ligue des droits de l'Homme* (LDH) call on the Parliament to delete article 20 (article 13's numbering changed during LPM's second reading). On December 10th, Reporters Without Borders denounces article 13's impact for the confidentiality of reporter's sources, as well as the lack of consultation on the provision.

- Despite the growing mobilization by civil society, media attention to the issue, and increasingly vocal opposition by a few MPs, the Parliament definitively adopts the Military Planning Law, along with article 20, on December 10th. The provision's proponents keep claiming that it brings new safeguards and suggest that critics are misinforming public opinion.

- On December 13th, a first coalition efforts finally emerges: Reporters Without Borders, FIDH, LDH and LQDN jointly write an open letter to the Parliament, calling on MPs to refer the law to the Constitutional Council (in France, 60 deputies or of 60 senators are needed to introduced a referral for *ex ante* constitutional review).

- A new petition is launched to relay the demand for a referral to the Constitutional Council. Within a few days, it gathers more than 80,000 signatures.

- At first, MPs opposed to article 20 appear confident they can meet the 60-member threshold. But on December 18th, after pressure by the conservative leadership who is afraid of appearing "soft on security" and refuses a joint-appeal with the Green Party, they have to renounce.

- On December 19th, the LPM is signed into law by President Hollande.

- In reaction to the promulgation of the law, the CNIL adopts on the same day an official position on article 20. While downplaying the

[73] *Avis n°5-2013 du Conseil national du numérique sur les libertés numériques.* Paris: Conseil national du numérique, Dec. 6, 2013. Available at: http://www.cnnumerique.fr/libertes-numeriques/.

fear of "massive surveillance" expressed by civil society groups, it nevertheless relayed their concerns, namely the lack of consultation, the fact that the text fails to clearly distinguish between communications content and metadata (article 20 referred to metadata through the the ambiguous terms "information and documents" inherited from the 1991 Wiretapping Act), and the risk that intelligence agencies might have direct access to telecom and hosting providers' infrastructures (with the law's unclear expression of "direct solicitation of the network"). The CNIL ends the document by pledging to be proactive in the drafting of article 20's implementation decree, on which it would be consulted.

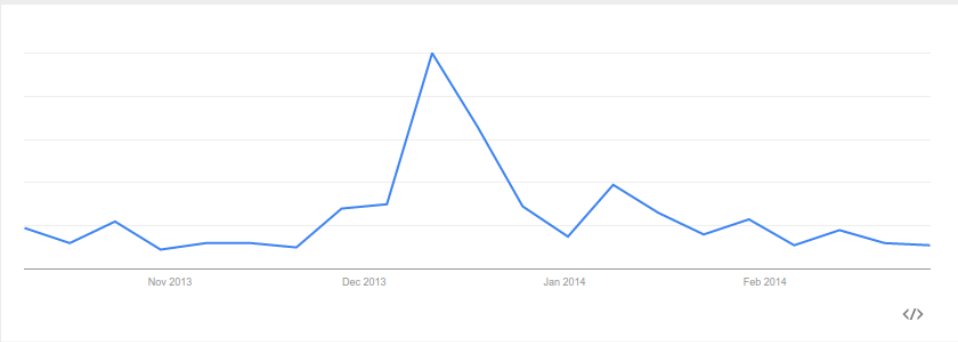

Figure 5: Volume of web searches in France for the term "*Loi de programmation militaire*" from October 2013 to February 2014, showing a peak during the civil society mobilization in December (Google Trends).

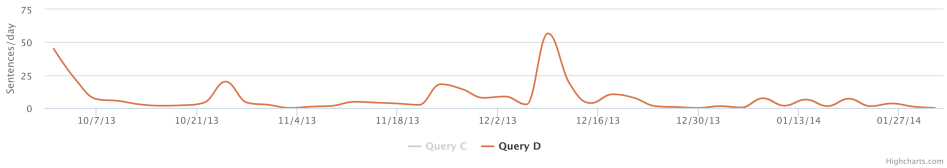

Figure 6: Number of sentences per day mentioning the term "*Loi de programmation militaire*" in French national online news sources from October 2013 to February 2014, also showing a peak of attention in December (MediaMeter).

Towards coordinated activism against Internet surveillance

This episode of contention around article 20 was late but dense. And despite its lack of expertise on LPM and its somewhat exaggerated denunciation of "generalized surveillance," the first episode of post-Snowden contention had at last led to a process of mobilization around Internet surveillance issues.

On the web page of the petition calling for referral to the Constitutional Council, an update was added on November 19th to denounce the opposition's political manoeuvres while stressing that, "for the first time in France, our action has led to the creation of an actual movement for the protection of our freedoms on the Internet." This may have been an overstatement, as there had been prior wide-ranging mobilizations –for instance against the "three-strikes" copyright law in 2009. But in recent memory, such a mobilization against Internet surveillance –even though it was largely improvised and resulted from immediate circumstances– was indeed a first. And it would bear fruition in the longer term.

Probably frustrated by their failure to react in time to Sueur's amendments (and to do so before rather than after industry groups like ASIC) –also finally realizing the need to build and share expertise around Internet surveillance and digital rights in general–, civil society groups created creation a new umbrella organization. Announced on the international "data protection day," it was called the *Observatoire des Libertés et du Numérique* (OLN).

OLN's initial members included organizations that often worked together on non-Internet issues –including LDH, a lawyers union (*Syndicat des avocats de France*) and a judges union (*Syndicat de la magistrature*). They were joined by two smaller research organizations devoted to the interplay of the digital sphere and privacy (CECIL and CREIS-Terminal). A few days later, LQDN –with its already established expertise on digital rights, its singular Internet-inspired political culture as well as its own international networks–, asked to join the coalition, thus becaming a new member of OLN. This *brokerage* – the "the production of a new connection between previously unconnected sites"–[74] would play a key role against the Intelligence Bill.

Besides this brokerage, another important process occurring over the course of the LPM mobilization was the *certification* of the anti-surveillance contention by institutions like CNIL or the French Digital Council (according to Tilly and Tarrow, certification occurs when an "external authority's signal of its readiness to recognize and support the existence and claims of a political actor).[75]

A year later –that is to say just before existing provisions on administrative access to metadata were set to expire–, the government adopted the implementation decree of LPM's article 20.[76] It aimed to prove its critics wrong. Though oversight was still crucially lacking, the decree adopted a restrictive interpretation of the Bill's broadly worded provisions: There would no be direct access to privately-owned infrastructures (servers and

[74]Tilly and Tarrow, *Contentious Politics*, p. 33.

[75]Tilly and Tarrow, *Contentious Politics*, p. 36.

[76]See *décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion*. The decree created a whole new chapter in the Code of Internal Security dedicated to the administrative access to metadata.

networks) and, save for the inclusion of geographic metadata provided for in the law, the scope of metadata would be left unchanged compared to the 2006 decree.

Even so, for the next few months after the adoption of LPM, the government would halt the path to legalization set forth by Urvoas. Post-Snowden contention was finally underway in France, and it was likely perceived to make any large-scale intelligence reform much more risky politically. At least in the short term...

3 A Long-Awaited Legalization: Passing the 2015 Intelligence Act

In the remainder of the paper, we finally come to the passage of the Intelligence Act. We show the key role of securitization in legitimizing intelligence reform, provide an overview of the text's key provisions before turning to the mobilization of civil society during the parliamentary debate.

3.1 From ISIS to Charlie: Reigniting the Debate

So what were the change in conditions that finally reduced the political cost of Intelligence Reform and (re)opened the path to wide-ranging legalization?

One key factor was undoubtedly the return of full-fledged securitization discourse in the summer of 2014, with the impressive military rise and media hype around the Islamic State in Iraq and Syria (ISIS).[77] Whereas the 2012 anti-terrorism law had been passed with relative discretion by the government, another one was introduced in great fanfare in July 2014.[78]

The law greatly reinforced the power of intelligence and police agencies by circumventing traditional criminal procedures. Its main Internet-related provisions included the extra-judicial censorship of content and the blocking of whole websites "inciting or apologizing for terrorism," the transfer of the incrimination for "inciting of apologizing for terrorism" from the Press Law (with its special procedural safeguards) to the Criminal Code, and administrative prohibition on leaving the territory (on intelligence-based allegations that they might try to join a foreign terrorist organizations). The law also contained measures not specific to terrorism, such as the extension of seizure powers to remotely-accessible computer equipments accessible from the police's own premises.

[77] Henry A. Giroux. "ISIS and the Spectacle of Terrorism: Resisting mainstream workstations of fear". *Philosophers for Change* (Oct. 7, 2014). Available at: https://philosophersforchange.org/2014/10/07/isis-and-the-spectacle-of-terrorism-resisting-mainstream-workstations-of-fear/.

[78] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

The law offered a first opportunity for OLN members to engage in coordinated action in their campaign against a Bill, sharing analysis and campaign tools, expanding their networks for international support. But it was eventually adopted with no substantial change on these issues the following November.

But on July 9th, 2014, just as the government was introducing the terrorism Bill before the parliament, President Hollande was convening a National Intelligence Council at the Élysée Palace. In the laconic press-release issued on that day, it was told that the Council had

> determined the strategic priorities of [intelligence] services and approved the legal, technical and human resources necessary to carry on these priorities.

That summer, the forecast started to look brighter for the Intelligence Bill. But what did other French institutions think?

Two month later in September, the so-called "report section" of the Council of State –formally distinct from its court section– issued its 2014 annual study focusing on "fundamental rights and the digital sphere."[79] Naturally, the report made several mentions of the Snowden disclosures. And it came strongly against the CJEU's *Digital Rights* ruling.

After presenting different possible interpretations of the *Digital Rights* decision, the Council's report went as far as stressing that, if the court were to unambiguously outlaw blanket data retention laws in future rulings, Member States still had the possibility of circumventing the court's case law by adopting an interpretative protocol to the Charter of Fundamental Rights.[80] The report did what the government had not even dared to do publicly. The idea was technically very simple but politically disastrous: Member states, the Council of State contended, could always go higher in the hierarchy of norms, and tweak the treaties to explicitly allow for such measures...

Except for this, the report sought to give some credit to the Council of State' self-proclaimed commitment to the protection of civil right against government abuse (grossly exaggerated, especially in the field of intelligence law). To that end, it called for instance on the adoption of special privacy protections for privileged professions such as journalists, lawyers or judges. It favored the regulation of international surveillance and advocated for a significant increase in the human and financial resources of the oversight body, which the report said should have "high-level competences" in engineering and data analysis.

[79] Jacky Richard and Laurent Cytermann. *Le numérique et les droits fondamentaux.* Les rapports du Conseil d'État. Conseil d'État, Sept. 9, 2014. Available at: http://www.ladocumentationfrancaise.fr/rapports-publics/144000541/index.shtml.

[80] Richard and Cytermann, *Le numérique et les droits fondamentaux*, p. 210.

In December 2014, Jean-Jacques Urvoas presented a yet another report written on behalf of the *Délégation parlementaire au renseignement*.[81] That DPR report started off by praising the LPM for entrusting it with enhanced oversight powers. It also sought ease concerns raised during the law's adoption, which it said had been "caricatural."

Again, the DPR report included a chapter calling for a reform of the intelligence legal framework. It started by welcoming the decision of the National Intelligence Council's "favorable echo" to the idea of intelligence reform and went on to restate three core justifications for a legislative overhaul: it would protect "individual freedoms," legitimize the activity of intelligence services, and protect people in intelligence community from legal insecurity.

The report also alluded to, and directly sought to influence, ongoing arbitrations on the scope of a unified law on intelligence activities. Against some who would have wanted a mere list of the technical capabilities open to intelligence services, Urvoas instead defended an ambitious bill that would also inscribe intelligence in the real of public policy by defining their missions (all of which should contribute to "preserving the rule of Law") and provide new safeguards and redress mechanisms for citizens. Most crucially, it called for an oversight commission with extended powers, including on surveillance operation occurring *outside* of the French territory by the DGSE.

Finally, it sought to distance French intelligence policy from that of the US. For instance, still the "intelligence reform," it warned against the public-private hybridization of US intelligence embodied by Snowden's former employer, Booz Allen Hamilton, calling for the upcoming statute to ensure that intelligence would remain under "the sole authority of the state against the whims of the private sector."

A whole other chapter focused on the "Snowden revelations," trying to draw lessons from the ongoing wave of disclosures. Among other things, it said Snowden had become the "useful idiot" of terrorist groups by undermining the secrecy and therefore the effectiveness of COMINT surveillance, stressing that this had in turn created a threat for "European sovereignty." It lamented that Europe was highly dependent on the NSA for its COMINT capabilities, stressing that this represented a threat to "European sovereignty" while noting that, "thankfully," the DGSE was in this respect "ever more autonomous." Following Pellerin's interviews, it also called on "public opinion to understand that the main factor for the alienation of individual freedom is the consented abandonment of their data" and stressed that "such a risk was far greater for the citizen than the activity of intelligence services." The "Snowden chapter" concluded with the following lines:

[81] Jean-Jacques Urvoas. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*. 2482. Assemblée nationale, Dec. 18, 2014. Available at: http://www.assemblee-nationale.fr/14/rap-off/i2482.asp.

> In the end, Mr. Edward Snowden's revelations have documented practices which were hitherto only known to small insiders circles. They have highlighted the acuteness of a clandestine threat that puts in danger both or political and economical model as well as our most fundamentals individual freedoms. Confronted with this, the answer lies not in undermining the defensive and offensive state capabilities in the field of intelligence but in inscribing them in a better framework (especially legislative) as well as in the construction of effective safeguards.[82]

Overall, the DPR 2014 report restated Urvoas and Vadillo's past arguments and justifications. But as evidenced by this quote, they were also slightly altered by post-Snowden contention. Even though the report never spared an opportunity to scorn at opponents in civil society, it also aimed to cast the Parliament as a defender of civil rights against other unnamed insider participants of the debate on intelligence reform.

Less than a month after the report's release however, on January 7$^{\text{th}}$ and 9$^{\text{th}}$, the murders of the Charlie Hebdo staff and Hypercacher shoppers would precipitate the legalization process. On January 21$^{\text{st}}$, during a press conference, now-Prime Minister Manuel Valls turned the long-awaited intelligence reform into an essential part of the government's political response to the Paris attacks. Presenting a package of "exceptional measures" that formed part of the government's proclaimed "general mobilization against terrorism," Valls said a new law was "necessary to strengthen the legal capacity of intelligence agencies to act" against that threat.

3.2 The Intelligence Act's Main Provisions on Internet Surveillance

The Intelligence Bill was finally presented on March 19$^{\text{th}}$ during another press conference. Behind Valls, the event's poster read: "Intelligence Law, protecting while respecting freedoms." Meanwhile, the justification regime crafted by Urvoas and Vadillo had made its way to the Bill's explanatory memorandum, which underlined the backwardness of the French intelligence framework, the need for intelligence to catch up on the technical capabilities of judicial investigations, the legal insecurity of intelligence professionals, etc.

Two days earlier *Le Figaro* had run a piece revealing what would become the bill's most contested provisions, and in particular the one allowing Internet traffic-scanning device aimed at detecting "weak signals" of terrorism (the so-caled "black boxes"). But against rising criticisms, Manual Valls swore there would be no "mass surveillance of citizens," that on the contrary "this Bill will prohibit[ed] it." On April 13$^{\text{th}}$, as the National Assembly

[82] Urvoas, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, pp. 136-137.

began examining the Bill through a fast-tracked procedure, he again contended that the government's proposal had "nothing to do with the practices revealed by Edward Snowden."

But didn't it?

A full analysis of the Intelligence Bill, which goes far beyond Internet surveillance, is beyond the scope of this (already-lengthy) paper.[83] But though the government made great effort to fit into the case law of the ECHR,[84] a quick glance at its main Internet-related provisions suggest Valls' statements are misleading. Many of them touch on issues that have been key to the policy debates raised by the Snowden disclosures, and several clearly do legalize techniques of large-scale surveillance:

General provisions

Compared to the 1991 Wiretapping Act, the 2015 Intelligence Act enacts an unprecedented extension of the scope of "intelligence-gathering techniques." Through article L. 811-3,[85] it also extends the number of objectives that can justify extra-judicial surveillance. These include:

- national independence, territorial integrity and national defense;
- major interests in foreign policy, implementation of European and international obligations of France and prevention of all forms of foreign interference;
- major economic, industrial and scientific interests of France;
- prevention of terrorism;
- prevention of: a) attacks on the republican nature of institutions; b) actions towards continuation or reconstitution of groups disbanded under Article L. 212-1; c) collective violence likely to cause serious harm to public peace;
- prevention of organized crime and delinquency;
- prevention of proliferation of weapons of mass destruction.

[83] A rough translation of the 2015 Intelligence Act from French to English can be found at the following address: https://wiki.laquadrature.net/French_Intelligence_Laws (archive).

[84] See, in particular, the section on the ECHR in the Bill's impact assessment: Gouvernement. *Étude d'impact du projet de loi n° 2669 relatif au renseignement.* République française, Mar. 18, 2015. Available at: http://www.assemblee-nationale.fr/14/projets/pl2669-ei.asp#P432_56763.

[85] Unless stated otherwise, all articles mentioned in this section are part of the Code of Internal Security.

Techniques of communications surveillance include telephone or Internet wiretaps (L. 852-1), access to identifying data and other metadata (L. 851-1), geotagging (L. 851-4) and computer network exploitation (L. 853-2), all of which are subject to authorization of a (renewable) duration of four months.

The government is allowed to extend by decree the number of law enforcement agencies who may conduct extra-judicial surveillance.[86] Finally, any telecom operator or hosting providers failing to comply with the data requests or other surveillance measures can be punished by a two-year imprisonment term and a €150,000 fine (article L. 881-2).

Oversight

The existing oversight commission, the CNCIS, is replaced by a new Commission called the "National Oversight Commission for Intelligence-Gathering Techniques" (*Commission nationale de contrôle des techniques de renseignement*, or CNCTR). According to the final version of the Intelligence Act –and much like the CNCIS–, it is comprised of nine members:

- four MPs designated by the Presidents of the Presidents of both chambers of Parliament;[87]
- two administrative judges and two judicial judges designated respectively by the Council of State and the *Cour de Cassation*;
- one technical expert designated by the telecom National Regulatory Authority (the addition of a commissioner with technical expertise was the main innovation).

The commissioners as well as their staff enjoy the highest security clearances so as to perform their duties.

Against Urvoas and Vadillo's early proposals of an oversight body with extended powers over intelligence agencies, the role of the CNCTR is restricted to the oversight of surveillance measures. The Commission has 24 hours to issue its *ex ante* non-binding opinion regarding the surveillance

[86]Beyond the intelligence community, the décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure opened the use of the surveillance techniques listed in the Intelligence Act to dozens of other agencies. The combined staff of these "second circle" agencies is over 45 000.

[87]Interestingly, the 2014 DPR report advocated against the inclusion of MPs in the new oversight body, in light of the increased parliamentary control of intelligence services achieved in recent years through the DPR.

authorizations delivered by the Prime Minister before surveillance begins,[88] except in cases of "absolute emergency" where it is simply notified of the surveillance measure within 24 hours upon deliverance (article L. 821-3).

As for *ex post* oversight, the CNCTR is supposed to have "permanent, comprehensive and direct access to records, logs, collected intelligence, transcripts and extractions" of collected data. It is able to conduct both planned and in the premises where these documents are centralized (article L. 833-2-2). If a irregularity is found, it can send to the Prime Minister a "recommendation" so that she can put an end to it.

One hugely significant exception to the CNCTR's oversight powers are the bulk of data obtained through data-sharing with foreign intelligence agencies (article L. 833-2-3). This exemption, which is all the more surprising considering the scale of data-sharing and the fact that data collected by foreign partners is likely to contain data on French residents, appears to be a pressing request from intelligence officials.[89]

Black boxes

As we will see, "black boxes" represents the most fiercely-debated provision of the bill. Article L. 851-3 of the Code of Internal Security provides that,

> for the sole purpose of preventing terrorism, automated processing techniques may be imposed on the networks of [telecom operators and hosting providers] in order to detect, according to selectors specified in the authorisation, communications that are likely to reveal a terrorist threat.[90]

This legalese attracted much discussions during parliamentary debates. The Minister of Defence, Jean-Yves Le Drian, explained that the goal was

[88] The non-binding nature of the CNCTR's *ex ante* oversight was criticized by the Bill's opponents. But as the 2014 DPR report had stressed a few weeks earlier, Urvoas and the government recalled that this was necessary to respect the Constitution's article 20 . According to the later, the government "shall have at its disposal the civil service and the armed forces." Since the CNCTR is organically part of the executive branch, the Prime Minister –as head of the government– supposedly cannot be bound by its decisions.

[89] In August 2013, *Le Monde* ran the following quote from a source at the DGSI: "We exchange all the time with foreign agencies, including with interlocutors of the DGSE such as the American NSA of the British GCHQ. A great part of our intelligence includes elements belonging to our partners; needless to say we won't let anyone land their hands on it." Jacques Follorou. *Le renforcement du contrôle se heurte à la coopération internationale entre services*. Aug. 22, 2013. Available at: http://www.lemonde.fr/societe/article/2013/08/22/le-renforcement-du-controle-se-heurte-a-la-cooperation-internationale-entre-services_3464714_3224.html.

[90] Full sentence in French: "*il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste*."

to detect "connections a certain hours, from certain places, on certain websites." In that case, the operational goal is to detect the IP addresses or telephone numbers of known terrorist suspects with potential recruits, or to spot those who try to connect to a "terrorist website." The Director of the DGSE, Bernard Bajolet, gave another example during a committee hearing, asserting that the goal was to "discern clandestine attitudes," alluding to the use of cryptographic and anonymizing tools (for instance using a proxy server).

As for the exact technical nature of these real-time traffic-scanning devices, critics of the proposal feared that the government would use potentially extremely intrusive technologies known as "Deep Packet Inspection" (DPI), which would anable the automatic analysis of all communications flowing trough the network.[91]. The government –this time through Interior Minister Bernard Cazeneuve, who complained about the "prevailing hubbub and media uproar"– said it would not use DPI. An implementation decree published in January 2016 suggest this may be true: black boxes will "only" monitor metadata (including recipient IP address), rather than the content of communications.[92] So in that sense –and assuming that the law is respected–, black boxes do not rely on "deep packet" inspection. But then again, metadata surveillance can often be considered more intrusive than the surveillance of communications content.[93] The computing tools that will be needed to sort though the packet headers flowing through the black boxes will necessarily be very similar in nature to DPI filtering.

Black boxes are authorized after an opinion by the CNCTR, for a duration of two months, as is the real-time collection of identifying data (article L. 851-3, for terrorism only). Their conformity with EU law –and in particular article 15 of the so-called eCommerce directive, which provides that Member States "shall not impose a general obligation on providers (...) to monitor the information which they transmit or store"–[94] remains dubious.

Computer Network Exploitation

The Act authorizes hacking as a method for intelligence gathering. Article L. 853-2 allows for:

[91] Deep Packet Inspection a form of computer network packet filtering that examines the data part (content) –and possibly also the header (or metadata)– of a packet as it passes an inspection point (source: Wikipedia).

[92] *Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.*

[93] Claudia Aradau and Tobias Blanke. "The (Big) Data-Security Assemblage: Knowledge and Critique". *Big Data & Society* 2.2 (Dec. 1, 2015). Available at: http://bds.sagepub.com/content/2/2/2053951715609066.

[94] Article 15 of the directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

- access, collection, retention and transmission of computer data stored in a computer system;
- access, collection, retention and transmission of computer data, as it is displayed on a user's computer screen, as it is entered by keystrokes, or as received and transmitted by audiovisual peripheral devices.

Considering the intrusiveness of computer hacking, the law provides that these techniques are authorized for a duration of thirty days, and only "when intelligence cannot be collected by any other legally authorized mean."

The Act also grants blanket immunity to intelligence officers who carry on computer crimes into computer systems located abroad (article 323-8 of the Penal Code). This, in turn, may contravene article 32(b) of the Budapest Convention on Cybercrime on the trans-border access to computer data.[95]

International surveillance

The Act also legalizes the DGSE's Internet surveillance apparatus developed since 2008 under a chapter on the "surveillance of international communications." International communications are defined as "communications emitted from or received abroad," that is to say, to put it more simply, going in or out of the country.

The legal regime created here is a complex one:

- For the collection of "international communications," the Prime Minister "designates" (rather than "authorizes") which network infrastructure (e.g. the cable-landing stations owned by telecom operators) are subject to large-scale interception (article L. 854-2-I).
- After collection, "when it appears" that both ends of the communications are coming from "technical identifiers that are traceable to the national territory" (e.g.: emitter and receiver are using French telephone numbers or IP addresses), article L. 854-1 provides that intercepted communications "shall be immediately deleted," unless the persons targeted are physically located abroad and either i) already covered by a national surveillance authorization or are ii) deemed to be a national security threat. However, given the transnational nature of Internet communications, and the fact that a communication between two French residents is likely to be routed in and out of French borders, one can doubt on the effectiveness of such a safeguard.

[95] See the interpretation of the Cybercrime Convention Committee: "In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b." *T-CY Guidance Note #3 Transborder access to data (Article 32).* T-CY (2013)7 E. Strasbourg: Council of Europe, Dec. 3, 2014. Available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V11.pdf, p. 7.

- For bulk analysis of intercepted metadata (what the Act calls "non-individualized *exploitation*" of metadata), the Prime Minister issues an one-year authorization specifying the purposes of such analysis and which intelligence agencies are in charge of conducting it (article L. 854-2-II). This seems to refer to the automated-scanning of intercepted metadata, similar to black boxes, but this time not restricted to anti-terrorism.

- For the exploitation of the *content* of communications or of their metadata, the Prime Minister issues a four-month authorization specifying the purposes justifying such analysis, the intelligence agencies in charge, as well as targeted geographic zones, organizations, groups of people or individuals.

The CNCTR is only notified of all authorizations related to international surveillance and can issue recommendations to the Prime Minister if irregularities are found.

Finally, the so-called Hertzian provision of the 1991 Wiretapping Act – originally created for bulk satellite interceptions – was carried by the Intelligence Act. Under this blanket provision which in the past has served to cover up for various illegal programs of communications surveillance, the collection and exploitation of wireless signals therefore remains completely devoid of safeguards (article L. 811-5). Because the exact content of the article never appeared in the Bill –which only relocated the existing provision in the Code of Internal Security–, it was completely overlooked during the parliamentary phase of the contention against the law and was rediscovered by civil society almost by surprise in April 2016. A constitutional challenge ensued, and the provision was eventually struck down by the French Constitutional Court on October 21st, 2016.[96]

Data retention periods

For national surveillance measures, once communications data are collected by intelligence agencies, retention periods are the following:

- Content (*correspondances*): 1 month after collection (for encrypted content, period starts after decryption, within the limit of 6 years after initial collection);

- Metadata: 4 years (compared to the LPM decree 3-year period).

[96]For a short overview of the history of the Hertzian provision and of the Constitutional Council's ruling, see: Félix Tréguer. *French Constitutional Council Strikes Down "Blank Check Provision" in the 2015 Intelligence Act.* Oct. 2016. Available at: http://verfassungsblog.de/french-constitutional-council-strikes-down-blank-check-provision-in-the-2015-intelligence-act/.

For international surveillance, retention periods depend on whether one end of the communication uses a "technical identifiers traceable to the national territory" or not, in which case the "national" retention periods are applicable, but they start after the first exploitation and no later than six months after collection (article L. 854-8). If both ends of the communication are foreign, the following periods apply:

- Content: 1 year after first exploitation, within the limit of 4 years after collection (for encrypted content, periods starts after decryption, within the limit of 8 years after collection);
- Metadata: 6 years.

Redress mechanism

The Act reorganizes redress procedures against secret surveillance, establishing –and this is one of the main innovation of the bill– the possiblity to introduce a legal challenge before the Council of State. The procedure is the following:

- Any legal person can introduce a complaint to the CNCTR, asking the oversight body to investigate whether or not she has been subject to illegal surveillance measures (article L. 833-4). The CNCTR can then only notify the plaintiff it has carried on necessary checks, "without confirming or denying" whether or not they have been spied upon.
- Only after taking this preliminary step, plaintiffs can appeal to the Council of State, who is competent in first and last resort. The same procedure is opened to the CNCTR when its investigations uncovered irregularities but only when, once notified by the CNCTR, the Prime Minister has failed to take appropriate action.
- Intelligence-related cases are adjudicated by a new, three-judge spcial court within the Council of State. The court's judges and their staff have security clearance and can access any piece of information collected by the CNCTR (initial authorization, collected transcripts, etc.). The Act provides that the right of the defense, and in particular the right to open justice, may be "accommodated" to protect classified information. In practice, much of the evidence presented by the government to justify the necessity and proportionality of the surveillance measure will remain hindered from the plaintiffs and her lawyers (article L. 773-2 of th Code of Administrative Justice).
- When the special court finds a surveillance operation to be illegal, it can (but is not obliged to) put an end to it and/or order the collected data to be destroyed (article L. 773-7 of the Code of Administrative

Justice). Without compromising state secrets, it can then inform the plaintiff that the government has carried an illegal act, and order the state to pay damages.

This redress procedure seems inspired by the so-called "closed-material procedure" established in the UK through the Justice and Security Act of 2013, which are criticized for their detrimental impact on defense rights.[97]

Moreover, international surveillance remains outside of the scope of the redress procedure, as was confirmed by a ruling of the Constitutional Council,[98], casting strong doubts on the compatibility of this *as hoc* legal regime with ECHR case law.

Whistleblowing and right to information

Finally, following a recommendation of the Council of State in its 2014 report, Urvoas passed an amendment turning the CNCTR into an internal whistle-blowing channel for intelligence officers. But the provision remains very limited in scope.[99]

Moreover, the Act increases the criminal repression of disclosures regarding the "existence of the deployment" of a given surveillance technique (article L. 881-1): Such unauthorized disclosures are punished by a two-year imprisonment term and a €150 000 fine (against a two-year term and a €30 000 fine before).

Lastly, the court rulings of the Council of State's special section and its general case-law will remain secret (article L. 773-7 of the Code of Administrative Justice).

All of these provisions affecting the right to information obviously fail to comply with international best-practices, such as those laid down in the Tschwane principles on national security and the right to information.[100]

[97] Didier Bigo et al. *National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges.* Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs PE 509.991. Brussels: European Parliament, 2014, p. 156. Available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282014%29509991.

[98] See *Décision n° 2015-722 DC du 26 novembre 2015*, §18: "*Considérant que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure ; qu'en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale.*"

[99] The range of abuses that can be reported are limited to criminal violations of the confidentiality of communications. Cases of active corruption, for instance, are not covered. What is more, a last-minute governmental amendment deleted the sentence granting potential whistleblowers the right to "testify about classified information, information that might harm the security of personnels, or undermine the missions of intelligence agencies." This creates huge legal insecurity for potential whistleblowers.

[100] See, in particular, principles 39 and 40 on internal whistleblowing channels and public

3.3 The Mobilization Against the Bill

By the time the Intelligence Bill was introduced in Parliament, civil society organizations such as those taking part in OLN had become more organized. They had already worked together on national security legislation with their common campaign against the Terrorism Law of November 2014, building expertise and engaging in coordinated action.

During the three-month long parliamentary debate on the Bill (April-June 2015), NGOs were able to lead the contention against the Bill, while benefiting from the support of variety of other groups and actors typical of post-Snowden mobilizations against surveillance. In this section, we present the network of actors mobilized against the Bill (see figure 7 and/or explore online at the following address: https://is.gd/cLkzqh).[101]

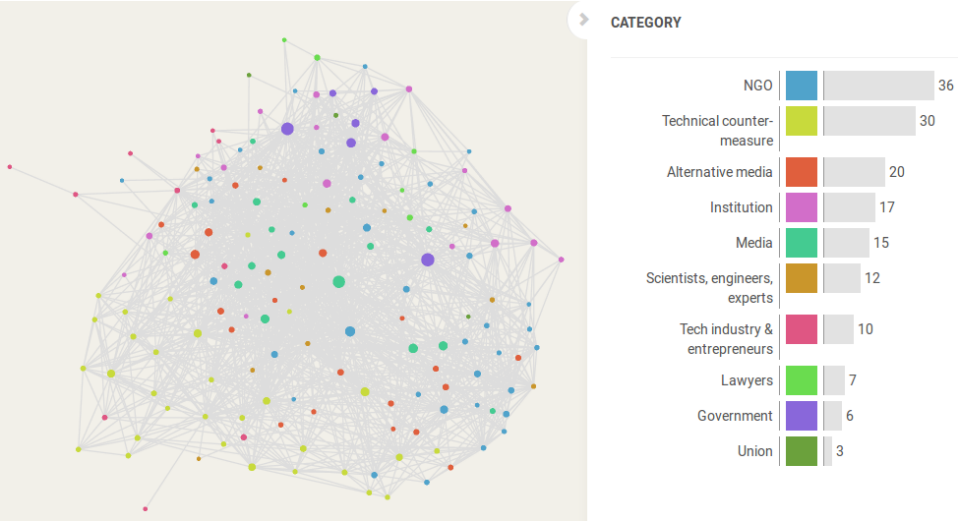

Figure 7: Web cartography of actors mobilized against the Intelligence Bill. Explore online at the following address: https://is.gd/cLkzqh.

disclosures as well as principle 28(b) on the publicity of court rulings. *The Global Principles on National Security and the Right to Information (Tshwane Principles)*. Open Justice Initiative, June 12, 2013. Available at: https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

[101] The Web cartography presented in figure 7 was obtained through web crawling (Hyphe) and visualization tools (Gephi and ManyLines) developed by Sciences Po's Medialab. For background on methodology used by the Hyphe crawler, see: Mathieu Jacomy et al. "Hyphe, a Curation-Oriented Approach to Web Crawling for the Social Sciences". *International AAAI Conference on Web and Social Media*. Köln, Germany: Association for the Advancement of Artificial Intelligence, May 2016. Available at: https://hal.archives-ouvertes.fr/hal-01293078.

Advocacy groups, lawyers, unions

This time, the mobilization of NGOs was quick and, in many respects, effective. OLN led the way in allowing joint analysis and coordinated action between human rights advocates (LDH, FIDH, etc.), digital rights activists (LQDN) and lawyers' associations (*Syndicat des avocats de France*, *Syndicat de la Magistrature*, etc.). It held a joint press conference in late-March, put together a campaign website (sous-surveillance.fr), organized a couple of street demonstrations (attended by only a few hundred supporters, which was enough to provide an illustration of the mobilization waging online). A phone-call and mailing campaign was also launched by LQDN and several other activist groups (LQDN reports close to a thousand calls passed to both chambers of Parliament through its online VOIP tool).

These groups succeeded in providing framing –and supporting legal analysis– of the Bill as a authorizing forms of "mass surveillance." They gathered support from leading international human rights organization like Amnesty and Human Rights Watch, whose French chapters took an active role in the opposition to the Bill. Digital rights international networks also mobilized in solidarity (EFF, EDRi, ACCESS, etc.), understanding the importance of the French case as one of the first post-Snowden attempt at legalizing mass surveillance. Once again, they received certification from major institutional actors (see below).

Finally, at the national level, they were backed by NGOs from other fields, like organizations of families of terrorism victimss, social workers, Act Up, motorcyclists organizations, a police union and several others. This broad dissemination of the contention helped rally audiences at the margin of traditional human rights advocacy.

Hackers & counter-measure providers

Another constituency mobilized against the Bill was a community of cryptography and free software organizations (TOR, Tails, etc.), as well as the French community Internet service providers (under the umbrella organization *Fédération FDN*).

These actors feature a strong technical know-how and a hacker (sometimes anarchist) political ethos. They relayed and sometimes directly contributed to the campaign of advocacy groups, providing technical expertise. Their Free Software, decentralized and encryption services were framed as non-profit, privacy-enhancing counter-measures to surveillance.

Digital entrepreneurs

Digital entrepreneurs added business argument against the Bill by framing human rights infringements as a deterrent for international clients as well as for research and development. "The Independent," as we might call them,

ranged from hosting providers and domain name registration services (like OVH and Gandi) to Software-as-a-Service startups (e.g. Cozy), all of which have connections with Free Software activist circles, digital rights NGO and institutions like the French Digital Council.

Their campaign against the Intelligence Bill was named "*Ni piegons, ni espions"*("neither pigeons nor spies"), alluding to the "*mouvement des pigeons*,"a 2012 campaign by startupers and investors against a fiscal measure elevating taxes on business sells. Their campaign website relayed their petition against the Bill –which gathered support of almost a thousand other small companies– as well as protest calls.

But what about large Silicon Valley firms and their French competitors? Trade group like ASIC also mobilized, but much less vocally than they had against the LPM in 2013. To the contrary of the full-fledged contention waged in the US or the UK, big US technology firms like Google or Microsoft declined to engage in the French debate, perhaps out of fear for being cornered for their double-speak on privacy and antagonizing even more French officials. As for their large French competitors, like Orange, SFR and others, their even greater dependence on and proximity with the state political elite ensured they would remain neutral bystanders.

Scientists, academia, experts

Actors with a strong technical capital like independent computer experts, social scientists, investigative bloggers specialized in intelligence matters (e.g. Zone d'Intérêt), former intelligence officers (e.g. Jacques Raillane, George Moréas) and the President of the Cryptographers' Reserve also contested the Bill.

One notable contending expert was Marc Trévidic, a famous anti-terrorism investigative judge. Early April, during a radio interview, he voiced the following concerns:

> An intelligence law should protect citizens not only against terrorism, but also against the State. We, in France, are doing neither. There is a total lack of oversight in this law. We are doing far less than we should (...). Frankly, the Prime Minister's room for maneuver is huge and the nation has no way of knowing whether something illegal will be done.[102]

Scientists also played a crucial role in validating the technical arguments put forward by activist groups. For instance, in late-April, a leading computer research institute, the INRIA, took a very unusual move by publishing

[102] *Marc Trévidic dénonce les dérives de la loi sur le renseignement.* RTL.fr. Apr. 7, 2015. Available at: http://www.rtl.fr/actu/societe-faits-divers/la-loi-sur-le-renseignement-entre-de-mauvaises-mains-est-une-arme-redoutable-estime-le-juge-marc-trevidic-7777296541.

a brief denouncing technical ineffectiveness and risk of abuse associated with Big Data surveillance.[103]

Institutional actors

Both national and international institutional actors played a important role in bringing certification to the Intelligence Bill's critics, supplying legal analysis and influencing the parliamentary debate.

The Commissioner for Human Rights at the Council of Europe, Nils Muižnieks, was for instance very vocal in the French media and wrote a letter to French Senators ahead of their vote on the Bill, pointing to the wide scope of the text and the lack of oversight.[104] The Human Rights Council of the United Nations also criticized the Bill in its periodic review of human rights in France, stressing it

> gives the intelligence agencies excessively broad, highly intrusive surveillance powers on the basis of broad and insufficiently defined objectives, without the prior authorization of a judge and without an adequate and independent oversight mechanism.[105]

The Organization for Security and Cooperation in Europe (OSCE) also voiced its concerns through its Representative on Freedom of the Media, Dunja Mijatović:

> While I fully respect any nation's right to protect its citizens, imprecise and intrusive provisions like these could stifle the right of journalists to seek, receive and impart information, as well as discussions about critical and sensitive issues through any mean of communication and without fear of surveillance

At the EU level, a handful of liberal Members of the EU Parliament voiced their opposition to the French Bill, in particular by asking the European Commission whether the Bill respected the Charter of Fundamental Rights.[106] But the Commission kicked into touch: "In accordance with its

[103] *Éléments d'analyse technique du projet de loi relatif au renseignement.* INRIA, Apr. 30, 2015. Available at: http://sciences.blogs.liberation.fr/files/265206918-note-interne-de-l-inria.pdf.

[104] Nils Muižnieks. *Lettre du Commissaire aux droits de l'homme du Conseil de l'Europe aux membres de la Commission des lois du Sénat français sur le projet de loi relatif au renseignement.* May 18, 2015. Available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH(2015)13&Language=lanFrench.

[105] *Concluding observations on the fifth periodic report of France.* CCPR/C/FRA/CO/5. Geneva: Human Rights Committee of the United Nations, July 21, 2015. Available at: https://archive.is/dUrgw.

[106] Nathalie Griesbeck et al. *Written question - French Government bill on intelligence.* E-005968/2015. European Parliament, Apr. 15, 2015. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2015-005968+0+DOC+XML+V0//EN.

standard practice," the answer read, "the Commission deems not appropriate to make comments on a Member State's national legislation as long as the domestic procedure has not been completed and the law in question adopted."

When asked on Twitter what the EU Commission would do to ensure that the Bill complied with the Charter of Fundamental Rights, Frans Timmermans, Vice-President of the Commission, was even more blunt: "The EU is not a fundamental rights super cop," he said, alleging that "The Charter is only binding on Member States when they apply EU law" (a highly debatable interpretation, considering the likely applicability of the eCommerce and ePrivacy directives to the Intelligence Act).

At the national level, the CNIL (data protection authority), the CNCDH (human rights watchdog) and the French Digital Council also logically certified the claims of NGOs. It was however more unusual to see former conservative politician Jacques Toubon, now holding the chair of ombudsman (*Défenseur des droits*), or Jean-Marie Delarue, a high-profile public servant and then sitting President of the CNCIS, publicly sharing their concerns. Other institutional opponents included several small left-wing parties and MPs from both sides of the aisle that actively fought against the Bill in the Parliament. A Special committee of the National Assembly conducting a prospective study on freedoms in the digital age also came out strongly against the Bill.

Alternative and mainstream media

Alternative media and journalists helped feed the contention by reporting on parliamentary debates, relaying the analysis of contentious actors and framing it for broader audiences. They included online publications specialized in Internet policy and tech news (*Next INpact*, *Numerama*, *reflets.info*), investigative newsrooms (*Mediapart*, *Arrêt sur image*) and mainstream outlets (*Le Monde*, *Libération*, *Telerama*, *Rue 89* and the more conservative *Le Figaro* or *La Croix*)

International mainstream media at the heart of the Snowden disclosures, such as The Guardian, also covered the debate on the French Bill. The New York Times even published a Op-Ed entitled "The French Surveillance State" which had a strong echo in France.[107]

3.3.1 How the Government Dealt With Contention

Contention against the Intelligence Bill was strong and sustained. It involved multiple actors with different action repertoires, expertise and audiences. As

[107]The Editorial Board. *The French Surveillance State*. Mar. 31, 2015. Available at: http://www.nytimes.com/2015/04/01/opinion/the-french-surveillance-state.html.

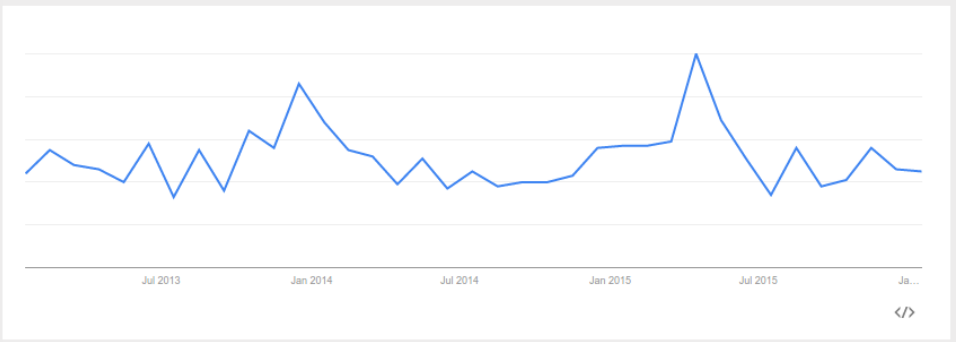

Figure 8: Volume of web searches comprising the terms "*Internet*" and "*surveillance*" in France from January 2013 to January 2016 (Google Trends).

a result, media attention to the issue of Internet surveillance was both longer and more intense than during previous episodes of contention (see figure 8).

Polls conducted in July 2015 –that is to say, at the end of the contentious episode– suggest that despite securitization, the mobilization somewhat managed to stir public concerns that the Bill undermined the protection of privacy and freedom of expression (for instance, 71% reported they were against the surveillance of their personal communications online).[108]

But how did the Bill's proponents respond to their contenders? Quite interestingly, they adopted a differential response to their opponents in civil society, the private sector, or in other public institutions.

Advocacy groups

Against the mobilization of human rights and digital rights NGO, the attitude was mainly dismissive. After hearing a handful of NGOs during committee hearings, Urvoas had to resist the growing citizen mobilization and ensure that the socialist majority would not break under public pressure.

When a campaign was launched calling on French citizens to get in touch with their elected representatives, Urvoas (and, most probably, Vadillo) took on drafting a response template for socialist MPs (after these emails were reported back to LQDN, the NGO quickly published counter-arguments).[109] In

[108] 82% of those interviewed said they were not ready to renounce the privacy for more security; 65% said they were hostile to the surveillance of their web-browsing habits even if was done only to prevent terrorism: 70% were against the mere "retention of their personal data on the Internet." *Les Français et la protection de la vie privée*. Paris: Institut CSA pour Ordre des Avocats de Paris, July 2015, p. 19. Available at: http://www.csa.eu/multimedia/data/etudes/etudes/etu20150715-Sondage-Francais-Protection-Vie-privee.pdf.

[109] Guillaume Champeau. *Loi Renseignement : des sondes directement chez les FAI et hébergeurs*. Numerama. Mar. 10, 2015. Available at: http://www.numerama.com/magazine/33120-loi-renseignement-des-sondes-directement-chez-les-fai-et-hebergeurs.

the text, they contradicted the notion that the Bill would establish a "generalized surveillance," claiming it would only legalize "individual, proportionate and temporary" intelligence-gathering activities. The "algorithm" –the term they used to refer to black boxes– would be used "only for metadata and strictly for the antiterrorist fight." And again, they distinguished the French way in the COMINT field to US practices:

> To the contrary of the United States, which resort to a massive and undifferentiated spying system, we prefer to focus our efforts on a surveillance limited to a few individuals ("*quelques individus*"), based on principles of efficiency and proportionality: the end does not justify all means.

A few days earlier, his report on the Intelligence Bill had used the same arguments. The lecturer in law mocked his opponents who had published legal analysis against the Bill, even fraying on philosophical grounds by distinguishing the Bill from the state of exception analyzed by Giorgio Agamben. The report claimed that French constitutional law and the European Convention immunized France against breached to the rule of law, adding:

> to the amateur exegetes who aim to address their own shortcoming by resorting to prejudice and to those of bad faith for whom suspicion is a substitute for reasoning, we must oppose a dispassionate analysis of the law.[110]

Opening the plenary debate at the National Assembly on April 13$^{\text{th}}$, Prime Minister Valls displayed a similar contempt against what he called the "fantasies" of civil society critics:

> Criticisms and postures evoking a French Patriot Act or the lingering smell of a political police are completely misleading and irresponsible, especially under the present circumstances. "A dangerous law": How can one assert such a lie?

Digital entrepreneurs

The criticisms voiced by ASIC members were met with similar disdain, in the rhetorical line first used by Fleur Pellerin. Google's lobbyists were invited for a committee hearing, but during, the rest of the discussion, the company's extensive collection of users' data was often cited as an example for the alleged widespread acceptance of Internet surveillance. On April

html.

[110] Jean-Jacques Urvoas. *Rapport de la commission des Lois sur le projet de loi relatif au renseignement.* Assemblée nationale, Apr. 2, 2015. Available at: http://www.assemblee-nationale.fr/14/rapports/r2697.asp, p. 41.

15th for instance, Bernard Cazeneuve, the Interior Minister, pointed during a National Assembly's plenary to the alleged double-dealing of the Bill' opponents, by offering to assess the comparative harms of private versus state surveillance:

> Internet services providers have in their possession our private data, and I am convinced that many of them use techniques that extraordinarily more intrusive for our own lives (...). This is not a problem for big international trusts (...). But when a government offers to prevent terrorism on the Internet, it is

The response to French independent digital companies was much more benevolent. For the government, their blend of human right and business arguments was harder to dismiss compared to that of the US corporations, and it felt compelled to accommodate their concerns –in particular those related to the black boxes that the government sought authority to install on their infrastructures. On April 13th, the government tabled a first amendment turning the contested article in a sunset provision expiring at the end of 2018 and committing to an assessment report to be presented to Parliament by July of that year.

On April 15th –the day of Cazeneuve's rant against the "big international trusts"–, his ministry convened the main representatives of the "*Ni Piegons, Ni Espions*" campaign. A few hours later, it followed-up on that meeting by tabling another "black box" amendment. The only substantial additional safeguard was that black boxes could not be authorized through the "emergency procedure." But the government also misleadingly framed the amendment as way to restrict the provision to the field of antiterrorism, even though such restriction had been there from the beginning, and claimed that hosting providers would be able to check on data processed by these black boxes when all what the amendment did was to restate that they would be the one installing the device on their networks.

This evasion tactic worked. Some of the biggest players of the business coalition immediately expressed their satisfaction, claiming that their concerns had been addressed by the amendment. Octave Klava, CEO of hosting provider OVH, still felt like the Bill "was not the right one" and that it would "have consequences for our daily lives." But, as he tweeted, he also felt that the amendment "answered the issues of trust that [the Intelligence Bill] raised for hosting providers in French data-centers." Others, like the hosting provider and domain name registrar Gandi, maintained their "citizen opposition" to the law, continued to support digital rights organization in their fight against the bill and to stress the negative impact of the law for their business operations in France. But the group as a whole seemed demobilized.

After this "conciliatory meeting," the "*Ni Piegons, Ni Espions*" campaign withered. Even though some of its most vocal participants would still

continue to go public about their opposition to the Bill, the campaign website was scarcely used thereafter, and only to relay protest calls initiated by NGOs. The threat expressed by some of them to "go into exile" never resurfaced, much less materialized. Overall, the success of the government's manoeuvre in defusing the initially strong and influential protest of digital entrepreneurs likely point to the lack of resolve, resources and/or expertise of these private actors to engage in a sustained political struggle against the government.

Institutional actors

The Bill's proponents kept their most-well argued response for institutional players. But again, they were dealt with selectively.

To the representatives of international or supranational institutions (Council of Europe, the UN's Human Rights Committee), French officials opposed mere indifference, as if they were trying to isolate the French public sphere from the global Snowden controversies. Mostly, it worked. Besides NGO and advocacy groups, they had little institutional relays in France, which more generally speaks about how little influence international human rights organizations have on liberal regimes.

To national institutional opponents, the Bill's proponents reacted with a blend of polite irritation and outright anger. The mildly-critical opinion of the CNIL –to which opposed MPs liked to refer to–, was never fully acknowledge for what it was, that is to say a partial certification of NGOs. Instead, they framed amendments bringing additional safeguards as a direct response to the CNIL's concerns, in a conciliatory attitude.[111]

Other institutional criticisms gave way to stark rebuttals. Following the CNCDH very critical opinion to the Bill, the Interior Minister published a fourteen-page letter refuting it point by point.[112] Addressed to Christine Lazergues, a professor of law and President of the CNCDH, the letter began with a cordial "*Chère Christine*" but went one in a much more vindictive way. Sometimes almost resorting to a satirical tone (e.g.: "the first part of the opinion calls on banning mass surveillance. The government fully subscribe to this principle"), sometimes falling into plain contempt (e.g.: ("this criticism, formulated very rapidly, is not backed up by any legal reference"),

[111] For instance, the CNIL had criticized the initial drafting of the black box provision, saying that it was misleading to pretend that metadata detected by the selectors were non-identifying, and that "anonymity" could only be lifted by requesting additional information from telecom operators. On April 15th, Urvoas justified one of his amendment substituting the term "identification" to that of "lifting of anonymity" in response to the CNIL.

[112] Bernard Caeneuve. *Réponse du ministre de l'Intérieur à l'avis de la Commission Nationale Consultative des Droits de l'Homme relatif au projet de loi sur le renseignement.* Paris: Ministère de l'Intérieur, Apr. 24, 2015, p. 14. Available at: http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Avis-de-la-CNCDH-sur-le-projet-de-loi-sur-le-renseignement.

the response was detailed and definitive. With rhetorical efficacy, it manifested the government legal services' deep knowledge of the law's origins and existing French and European case-law, even though it sometimes misrepresented them with a high degree of self-assurance.[113] The sharp tone of the response perhaps owed to the fact that many CNCDH commissioners came from civil society, and that indeed the essence of the CNCDH opinion was very similar to the criticisms of NGOs.

3.3.2 Impact of the Contention Against the Bill

If the attitude towards opponents ranged from dismissal and indifference to tactical conciliation, what was influence did contention have on the final text? Overall, both the Bill's rapporteurs and the government stood firm.

Urvoas played a particularly pivotal and interesting role in managing the parliamentary process and dealing with contention. In the line of the DPR report released in December 2014, Urvoas framed its role as that of the moderate. Defending the Parliament's prerogatives, he and his Senate counterpart, the conservative Philippe Bas, worked to make the Bill more detailed and balanced by reinforcing safeguards.[114] As already mentioned, Urvoas was the one introducing the whistleblowing provision. He also reinforced the prerogatives of the oversight commission, for instance by clarifying that the latter shall have "the human and technical resources needed to fulfil its missions and the corresponding funds" (article L. 832-3), or by subjecting black boxes and real-time access to metadata to *ex ante* oversight.

Overall, amendments to the Bill were significant but marginal corrections. Their aim was to improve the law's resilience to subsequent litigation and to accommodate some concerns, some of which Urvoas may have sincerely shared, though he was never too vocal about them. As a fine political tactician loyal to Prime Minister Valls, he always protected the government's red lines during the parliamentary debate. On a few occasions, he had to go against his own inclinations (and those of the Council of State), for instance by leaving leave foreign surveillance, e.g. surveillance operations conducted outside of the French territory, completely unregulated.

But Urvoas also acted as an missionary of the deep state, sometimes

[113]For instance, the letter misleadingly asserted that the case-law of both the CJEU and the ECHR held that access "tend to hold that metadata represent a lesser interference in the right to privacy than the interception of the content of communications." To back up these claims, Cazeneuve referred to the CJUE *Digital Rights* ruling (§39) and the ECHR's *PG and JH v. United Kingdom* ruling (§42), both of which more accurately take the position that interferences are different in *nature* rather than in *degree*. The *Digital Rights* ruling stresses that the retention of metadata "is a particularly serious interference. "

[114]Urvoas, *Rapport de la commission des Lois sur le projet de loi relatif au renseignement*; Philippe Bas. *Rapport de la commission des Lois sur le projet de loi relatif au renseignement*. 460. Sénat, May 20, 2015. Available at: http://www.senat.fr/rap/l14-460/l14-460.html.

even against the official position of the government. At the very end of the debate, he for instance inserted an amendment responding to a demand Bertrand Bajolet, the Director of the DGSE, during a committee hearing: the provision aimed to legalize the surveillance of non-French residents temporarily located on the French territory, without any independent oversight –apparently another alegal practice of the DGSE. The much-criticized amendment was an embarrassment for the government who eventually had to fight for its withdrawal.[115]

Similarly, during late-March committee hearings, Urvoas was likely the person responsible for convening the company Blue Coat Systems, the infamous US company most-known for supplying the Syrian regime with surveillance capabilities and a likely contender in a future "black box" public tender, whose name appeared in a parliamentary agenda released on March 24$^{\text{th}}$.[116] After public outcry, the hearing was called off the next day without any convincing explanation. One possible reason for the initial invitation is that the Bill's rapporteur sought to gather technical arguments in favor of "Big Data" surveillance techniques ahead of the debate.

Overall, contention played an important role in making such moves politically impossible and barring amendments that would have given intelligence agencies even more leeway than originally afforded by the Bill (some conservative MPs, in particular, sought to reclaim their contested status as the "tough-on-security" party). Whereas the government hoped for an "*union sacrée*" in favor of the Bill, contention managed to fracture the initial display of unanimity. MPs from across the political spectrum, including many among both socialist and conservative ranks, fought against the Bill. But this vocal minority was much too small to prevent the adoption of the Bill: In the end, the Bill was adopted with 438 votes in favor, 86 against and 42 abstentions at the National Assembly and 252 for, 67 against and 26 abstentions at the Senate.

A final stage in the opposition to the Bill was its legal review by the Constitutional Council. This time, to the contrary of the LPM, there was broad political consensus that a referral was necessary. Early on, in the face of widespread criticism, President Hollande had even committed to introduce his own referral.[117] In the end, 106 *députés*, and the President of the Senate logged their appeal to the Council, while a dozen of NGOs, lawyers and

[115] Franck Johannès. *Renseignement : l'amendement de dernière minute qui embarrasse le gouvernement*. Le Monde.fr. June 20, 2015. Available at: /societe/article/2015/06/20/renseignement-le-cas-a-part-des-etrangers_4658456_3224.html.

[116] Andréa Fradin. *Loi renseignement : l'Assemblée décommande Blue Coat, dont les machines fliquent le Web syrien*. Rue89. Mar. 25, 2015. Available at: http://rue89.nouvelobs.com/2015/03/25/loi-renseignement-lassemblee-decommande-blue-coat-dont-les-machines-fliquent-web-syrien-258376.

[117] *Loi sur le renseignement: François Hollande va saisir le Conseil constitutionnel*. L'Express. Apr. 19, 2015. Available at: http://www.lexpress.fr/actualite/politique/loi-sur-le-renseignement-hollande-va-saisir-le-conseil-constitutionnel_1672751.html.

trade groups also filed amicus briefs. Scholars from France, Belgium, the UK and the US –among which social theorist Zygmunt Bauman– even wrote an open letter to the judges: "after the revelations of Edward Snowden," read the letter, "what the world expects from France is a totally different policy giving credit to the promises of emancipation offered by an Internet that is true to the spirit of the Enlightenment."[118]

In its ruling of July 23rd, the Constitutional Council validated the law.[119] The only significant rebuttal was on a point raised not by MPs but by advocacy and lawyers' groups in an amicus brief, namely the fact that the details of the "international surveillance" provision were to be included in a secret implementation decree. The Council struck down the provision for failing to comply with the Parliament's constitutional duty to lay down appropriate civil rights safeguard through legislative statute. This forced lawmakers to adopt a another Bill on "the surveillance of international communications" in the Fall of 2015,[120] but by then –and despite the highly controversial nature of the these provisions aimed to legalize the DGSE's large-scale surveillance capabilites– the mobilization and media attention had faded.

3.4 More Securitization, More Surveillance

By the time the French government was ready to roll out the 2015 Intelligence Act with the adoption of its main implementation decrees, terrorism had struck again. The Paris attacks of November 13th, 2015 prompted the government to declare the "state of emergency," conducting more that 3000 extra-judicial house raids as well as searches and seizures in the following weeks –almost of all of which included the seizure (copy) of all data stored on computing devices found on the targets' premises.

In the aftermath of the attacks, government officials refused any critical examination of French intelligence policies, despite the fact that, once again, several of the attackers had been previously identified and monitored. Against the claims of former intelligence officials that there had been a structural deficit in the resource allocated to human intelligence-gathering compared to COMINT,[121] an unnamed government official quoted in *Le*

[118] *Lettre ouverte aux membres du Conseil constitutionnel.* July 20, 2015. Available at: https://blogs.mediapart.fr/edition/les-invites-de-mediapart/article/200715/lettre-ouverte-aux-membres-du-conseil-constitutionnel.

[119] *Décision n° 2015-713 DC du 23 juillet 2015*.

[120] *Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.*

[121] Jacques Follorou. *Renseignement : histoire d'une révolution avortée.* Feb. 5, 2016. Available at: http://www.lemonde.fr/police-justice/article/2016/02/04/renseignement-histoire-d-une-revolution-avortee_4859309_1653578.html; Michel Deléan and Louise Fessard. *L'antiterrorisme est à la peine depuis 2008.* Mediapart. Nov. 14, 2015. Available at: https://www.mediapart.fr/journal/france/141115/l-antiterrorisme-est-la-peine-depuis-2008?onglet=full; Michel Déléan. *Un ex-directeur de la DGSE: «On a baissé la garde sur le renseignement humain».* Mediapart. Nov. 20, 2015. Available at: https:

Monde asked for more surveillance powers, claiming that

> (...) because of to legal rules that prohibit, in particular, the massive collection of data which would allows for the real-time monitoring of these [whose name are on a watchlist for suspicious terrorism-related activities] (...). By aggregating information and using a powerful algorithm that we already know, we would be able to monitor, in real time, these 11 700 people. By combining databases for social security, terrorism, common law or any other signal collection form, we would have the means of triangulation to make connections and capture weak signals.[122]

Forty years after the SAFARI affair and in a country still under a profound shock, such a proposal went relatively unnoticed. As it turned out, it was part of a power struggle between some in the DGSI and the CNCTR, the oversight commission. A week after the attacks, the newly-created CNCTR said it was issuing opinion "days and nights" on surveillance authorizations,[123] but according to some sources in security services, such oversight still created too much bureaucratic hurdles. *Le Monde* would later explain that the head of CNCTR –Francis Delon, a former long-serving national security official in the Prime Minister's office– was standing in the way of those in domestic intelligence agencies who sought "simplified procedures" to spy on people on the terrorist watchlist, in particular for real-time access to metadata.[124]

This is interesting, because Delon's nomination as a President of the CNCTR had been criticized by civil society groups who feared his insider status made him much too close to intelligence and security circles.[125] But so far, Delon has sought to prove its critics wrong, apparently making strong displays of independence in order to preserve the legitimacy of his under-resourced institution. This can be seen as another outcome of the wide-ranging mobilization against the Bill.

However, the Interior Ministry eventually had its way. After the 2016 Nice Attack, the Intelligence Act's provision allowing for real-time access

//www.mediapart.fr/journal/france/201115/un-ex-directeur-de-la-dgse-baisse-la-garde-sur-le-renseignement-humain?onglet=full.

[122] Jacques Follorou. *Les failles de la lutte antiterroriste.* Nov. 20, 2015. Available at: http://www.lemonde.fr/attaques-a-paris/article/2015/11/19/les-failles-de-la-lutte-antiterroriste_4813166_4809495.html.

[123] Andréa Fradin. *Le surveillant des espions « a rendu des avis nuit et jour ».* Rue89. Nov. 18, 2015. Available at: http://rue89.nouvelobs.com/2015/11/18/surveillant-espions-a-rendu-avis-nuit-jour-262170.

[124] Jacques Follorou. *Tensions autour du contrôle du renseignement.* Le Monde. Mar. 5, 2016. Available at: http://www.lemonde.fr/societe/article/2016/03/05/tensions-autour-du-controle-du-renseignement_4877127_3224.html.

[125] Pierre Alonso and Willy Le Devin. *Francis Delon trop près de ses sources.* Sept. 15, 2015. Available at: http://www.liberation.fr/france/2015/09/15/francis-delon-trop-pres-de-ses-sources_1383279.

to metadata was extended by a Bill of the state of emergency to cover individuals not only "identified as a [terrorist] threat" but "likely to be related to a threat" or who simply belong to "the entourage" of individuals "likely related to a threat". According to La Quadrature du Net, this means that the provision can now potentially cover "hundreds or even thousands of persons (...) rather than just the 11 700 individuals" reported to be on the French terrorism watchlist."

More securitization is to be expected.

Right after the November Paris attacks, someone leaked to the press internal document from the ministry of the Interior. It summarized the wish-list of law enforcement agencies in the fight against terrorism. The document went on to contemplate banning open WiFi networks and anonymizing tools like the TOR network.[126] The Prime Minister eventually had to refute that such proposals were being seriously considered.

But since then, the Parliament has passed a new terrorism law vastly expanding the powers of prosecutors against those of independent judges, for instance by allowing them to order measures such as computer network intrusion without having to get approval from an independent judge.[127] Urvoas, who was promoted to the prestigious position of Minister of Justice in January, was responsible for the Bill.

When *Le Monde* published the quote of this unidentified government official advocating for the massive interconnection of public databases, an investigative journalist speculated that US company Palantir was a likely candidate for supplying this "powerful algorithm that we already know." He also noted that Palantir had recently started bidding for Big Data public tenders and that it was recruiting people with background in the administrative elite to roll-out an intense public relations campaign.[128] In October 2016, it was confirmed that Palantir had started training DGSI agents to the use of its Big Data tools.[129]

Also, in January 2016, the National Intelligence Council called on "deepening the internal and external action of intelligence agencies" and "reinforcing the pooling of their resources," which likely meant increasing the use of DGSE capabilities for domestic intelligence, which may raise legitimate con-

[126] Laurent Borredon. *La liste musclée des envies des policiers*. Dec. 5, 2015. Available at: http://www.lemonde.fr/attaques-a-paris/article/2015/12/05/la-liste-musclee-des-envies-des-policiers_4825245_4809495.html.

[127] *Projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, n° 3473, déposé le 3 février 2016*.

[128] kitetoa. *Palantir et la France : naissance d'une nouvelle théorie abracadabrantesque ?* Nov. 19, 2015. Available at: https://reflets.info/palantir-et-la-france-naissance-dune-nouvelle-theorie-abracadabrantesque/.

[129] Jacques Cheminat. *Big Data : la DGSI se rapproche de l'américain Palantir*. Oct. 2016. Available at: http://www.silicon.fr/big-data-la-dgsi-se-rapproche-de-palantir-161283.html.

cerns considering the shortcomings of these capabilities' legal basis.[130]

Lastly, threats against the right to encryption have become a recurring feature in securitization discourses since the Charlie Hebdo attacks.[131] Recently, the head of the DGSI, Patrick Calvar, commented about the March 2016 Brussels attacks that "even an interception would not have allowed to uncover the plot since communications were encrypted and nobody was able to break that encryption." The only solution to this "well-known problem," he claimed, is the adoption of new legal constraints aimed at forcing decryption capabilities onto providers.[132] New crackdowns in this field are to be expected in the coming months.

Conclusion: Resisting Rule by Law and the Snowden Paradox

Although the rhythm and scale of the disclosures unleashed by Edward Snowden have been drying up in the past months, the whistleblower's legacy will be enduring for anti-surveillance contention in the US, the UK, Germany, France, Brazil and many other countries in the years to come.

As we have seen, in a country like France, the global debate sparked by these disclosures played a vital role in mobilizing human rights advocates and other civil society groups that had previously overlooked the crucial stakes of secret state surveillance. One sign of the growing expertise and readiness of activists and human rights lawyers to tackle this issue is the number of legal challenges currently pending both before French and European courts against the 2015 Intelligence Act. Another is their growing inclusion in

[130] See 3.2.

[131] Marc Rees. *Deux députés s'attaquent au chiffrement.* Mar. 1, 2016. Available at: http://www.nextinpact.com/news/98821-deux-deputes-sattaquent-au-chiffrement.htm.

[132] These statements were made during a parliamentary hearing on May 10th, 2016: "We are facing a well-known problem that is only increasing: that of encryption," Calvar explained to the Defense Committee of the National Assembly. Talking about the Brussels attacks of March 2016, he added: "We're up against very structured organizations, very hierarchical, very militarized, comprised of individuals communicating with their command center, asking for instructions about actions to be taken and, in some cases, technical advice. Such communication is, let me repeat, permanent and no interception was conducted. But even an interception would not have allowed to uncover the plot since communications were encrypted and nobody was able to break that encryption. I will remind you of the conflict between Apple and the Federal Bureau of Investigation: Considering the power of the latter, one can see that we are facing a major issue that goes well beyond national borders." Later during the hearing, he came back to the matter: "In the field of interception, we are facing an enormous mass of data as well as the issue of encryption. Tomorrow, iPhones will use random encryption. I believe that the only way to solve this problem is to force providers." *Audition de M. Patrick Calvar, directeur général de la sécurité intérieure.* Compte rendu n°47. Paris: Assemblée Nationale, Commission de la Défense Nationale et des forces armées, May 10, 2016. Available at: http://www.assemblee-nationale.fr/14/cr-cdef/15-16/c1516047.asp.

the transnational networks of post-Snowden contention formed by NGOs, lawyers' groups and international human rights organizations such as the UN's Human Rights Council or the Council of Europe.

From the perspective of state authorities, these leaks led to a tough dilemma. On the one hand, they exposed these surveillance programs to advocacy and strategic litigation, thereby reinforcing the need to secure their legal basis. On the other, they made such a reform politically risky and unpredictable. It was only with the rise of the Islamic State as a national security threat from June 2014 on, and most importantly the Paris attacks of January 2015, that securitization discourse could be re-activated to promote the legalization of illegal large-scale surveillance capabilities.

France's passage of the 2015 Intelligence Act makes it an "early-adopter" of post-Snowden intelligence reform among liberal regimes. But lawmakers in several other European countries are now following suit. The British Parliament is currently debating the much-criticized Investigatory Powers Bill.[133] The Dutch government has recently adopted its reform proposal, which has also raised strong concerns.[134] The Polish government has announced plans to expand the access of law enforcement agencies to communications data, amid heated condemnations of the regime's "orbanization."[135] And in Germany, the Bundestag's Interior Committee will soon start working on amendments to the so-called "G-10 law," which regulates the surveillance powers of the country's intelligence agencies.[136]

Each country knows its own specific context, and post-Snowden contention around intelligence reform will most likely have different outcomes according to these varying contexts. As Bigo and Tsoukalas write,

> The actors never know the final results of the move they are doing, as the result depends on the field effect of many actors engaged in competitions for defining whose security is important, and of different audiences liable to accept or not that definition.[137]

These field effects are exactly what made post-Snowden intelligence reform hazardous for intelligence officials and their political backers. So it may

[133] Matt Burgess. *Investigatory Power Bill: UN warns UK's plans 'undermine' the right to privacy.* Wired UK. Mar. 9, 2016. Available at: http://www.wired.co.uk/news/archive/2016-03/09/un-privacy-ip-bill-not-compliant-international-law.

[134] *Dutch govt approves new wiretapping legislation.* Telecompaper. Apr. 18, 2016. Available at: http://www.telecompaper.com/news/dutch-govt-approves-new-wiretapping-legislation--1138892.

[135] Wiktor Szary. *Poles rally against new surveillance law amid 'Orbanisation' fears.* Jan. 23, 2016. Available at: http://www.reuters.com/article/us-poland-protests-idUSKCN0V10JV.

[136] Thorsten Wetzling. *The Key to Intelligence Reform in Germany.* stiftung neue verantwortung, Mar. 2, 2016. Available at: http://www.stiftung-nv.de/publikation/key-intelligence-reform-germany.

[137] Bigo and Tsoukala, *Terror, Insecurity and Liberty*, p. 5.

be that, in these other countries, human right defenders will have greater success than their French counterparts in defeating the false "liberty *versus* security" dilemma, framing strong privacy safeguards and the rule of law as core components of individual and collective security. However, the British debate on the 2016 Regulation of Investigatory Powers Bill, or the US' tepid reform of the PATRIOT Act in June 2015, indicate that the case of France is likely more telling than its decrepit political institutions may suggest. This is the "Snowden paradox": In the midst of unprecedented contention against Internet surveillance, ongoing reforms only serve to legalize practices of massive, suspicionless surveillance.

In the same way 9/11 brought an end to the controversy on the NSA's ECHELON program and paved the way for the adoption of the PATRIOT Act, the threat of terrorism and associated processes of securitization now tend to hinder the global episode of contention opened by Edward Snowden in June 2013. Securitization leads to a "chilling effect" on civil society contention, and makes legalization politically possible. This in turn leads to a "ratchet effect" in the development of previously illegal deep state practices and, more generally, of executive powers.

Fifteen years after 9/11, the French intelligence reform thus stands as a stark reminder of the fact that, once coupled with securitization, "alegality" and national security become two convenient excuses for legalization and impunity, allowing states to navigate the legal and political constraints created by human rights organizations and institutional pluralism. This is yet another "resonance" of the French Intelligence Act with the PATRIOT Act.[138]

In that respect, Urvoas is right: The Intelligence Act of 2015 is neither Schmitt's nor Agamben's states of exception. But because it is "legal" or includes some oversight and redress mechanisms does not mean that large-scale surveillance and secret procedures *do not* represent a formidable challenge to the rule of law. Rather than a state of exception, legalization carried on under the guise of the reason of state amounts to what Sidney Tarrow calls "rule *by* law," that is the reinforcing of executive powers through "legal manipulation under the umbrella of the rule of law."[139] In his study of the US "war on terror,", he writes:

> Is the distinction between rule of law and rule by law a distinction without difference? I think not. First, rule by law convinces both decision makers and operatives that their illegal behavior is legally protected (...). Second, engaging in rule by law provides a defense against the charge they are breaking the law. Over time,

[138]Pierre-Antoine Chardel, Robert Harvey, and Hélène Volat. "The French Intelligence Act: Resonances with the USA PATRIOT Act". Trans. by Ashar Foley. *Technology Science* (Mar. 15, 2016). Available at: http://techscience.org/a/2016031501/.

[139]Tarrow, *War, States, and Contention*, p. 245.

> and repeated often enough, this can create a "new normal," or at least a new content for long-legitimates symbols of the American creed. Finally, "legalizing" illegality draws resources and energies away from other forms of contention (...).[140]

The same process is happening with regards to present-day state surveillance: Large-scale collection of communications and Big Data preventive policing are becoming the "new normal." At this point in time, it seems difficult to argue that post-Snowden contention has hindered in any significant and lasting way the formidable growth of surveillance capabilities of the world's most powerful intelligence agencies.

And yet, the jury is still out. Post-Snowden contention has documented state surveillance like never before, undermining the secrecy that surrounds deep state institutions, prevents their democratic accountability, and helps sustain taken for granted assumptions about them. It has provided fresh political and legal arguments to reclaim privacy as a "part of the common good,"[141] leading courts –and in particular the CJEU and the ECHR– to admit several cases of historic importance which will be decided in the coming months.

Judges now appear as the last institutional resort against large-scale, suspicionless surveillance. If litigation fails, the only possibility left for resisting it will lie in what would by then represent a most transgressive form of political action: upholding the right to encryption and anonymity, and more generally subverting the centralized and commodified technical architecture that made such surveillance possible in the first place.

Books & Academic References

Aradau, Claudia and Tobias Blanke. "The (Big) Data-Security Assemblage: Knowledge and Critique". *Big Data & Society* 2.2 (Dec. 1, 2015). Available at: http://bds.sagepub.com/content/2/2/2053951715609066.

Bigo, Didier and Anastassia Tsoukala, eds. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. 1 edition. London; New York: Routledge, 2008.

Chardel, Pierre-Antoine, Robert Harvey, and Hélène Volat. "The French Intelligence Act: Resonances with the USA PATRIOT Act". *Technology Science* (Mar. 15, 2016). Available at: http://techscience.org/a/2016031501/.

[140] Tarrow, *War, States, and Contention*, pp. 165-166.

[141] David Lyon. *Surveillance After Snowden*. Polity Press, 2015. 120 pp., p. 99.

Cheminat, Jacques. *Big Data : la DGSI se rapproche de l'américain Palantir*. Oct. 2016. Available at: http://www.silicon.fr/big-data-la-dgsi-se-rapproche-de-palantir-161283.html.

Errera, Roger. "Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques". *Revue trimestrielle des droits de l'Homme* 55 (2003), pp. 851–870.

Giroux, Henry A. "ISIS and the Spectacle of Terrorism: Resisting mainstream workstations of fear". *Philosophers for Change* (Oct. 7, 2014). Available at: https://philosophersforchange.org/2014/10/07/isis-and-the-spectacle-of-terrorism-resisting-mainstream-workstations-of-fear/.

Hassoux, Didier, Christophe Labbe, and Olivia Recasens. *L'espion du président*. Paris: Robert Laffont, 2012.

Hayez, Philippe. ""Renseignement": The New French Intelligence Policy". *International Journal of Intelligence and CounterIntelligence* 23.3 (June 8, 2010), pp. 474–486.

Jacomy, Mathieu et al. "Hyphe, a Curation-Oriented Approach to Web Crawling for the Social Sciences". *International AAAI Conference on Web and Social Media*. Köln, Germany: Association for the Advancement of Artificial Intelligence, May 2016. Available at: https://hal.archives-ouvertes.fr/hal-01293078.

Joinet, Louis. *Mes raisons d'État: Mémoires d'un épris de justice*. La Découverte, 2013.

Lyon, David. *Surveillance After Snowden*. Polity Press, 2015.

Marzouki, Meryem. "« Non à Edvige » : sursaut ou prise de conscience ?" *Plein droit* 80 (Mar. 1, 2009), pp. 21–26. Available at: http://www.cairn.info/resume.php?ID_ARTICLE=PLD_080_0021.

Tarrow, Sidney. *War, States, and Contention: A Comparative Historical Study*. 1 edition. Ithaca ; London: Cornell University Press, 2015.

Tilly, Charles and Sidney Tarrow. *Contentious Politics*. 2nd edition. New York: Oxford University Press, 2015.

Tréguer, Félix. *French Constitutional Council Strikes Down "Blank Check Provision" in the 2015 Intelligence Act*. Oct. 2016. Available at: http://verfassungsblog.de/french-constitutional-council-strikes-down-blank-check-provision-in-the-2015-intelligence-act/.

Policy Reports

22e rapport d'activité 2013-2014. Paris: CNCIS, 2015. Available at: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101/0000.pdf.

Audition de M. Bernard Bajolet, directeur général de la sécurité extérieure, sur le projet de loi relatif au renseignement. Compte rendu de séance n°47. Paris: Assemblée nationale, commission de la défense nationale et des forces armées, Mar. 24, 2015. Available at: http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415047.asp#P3_69.

Audition de M. Patrick Calvar, directeur général de la sécurité intérieure. Compte rendu n°47. Paris: Assemblée Nationale, Commission de la Défense Nationale et des forces armées, May 10, 2016. Available at: http://www.assemblee-nationale.fr/14/cr-cdef/15-16/c1516047.asp.

Audition du préfet Érard Corbin de Mangoux, Directeur général de la sécurité extérieure (DGSE) au ministère de la Défense. Compte rendu n°56. Paris: Assemblée nationale, commission de la défense nationale et des forces armées, Feb. 20, 2013. Available at: http://www.assemblee-nationale.fr/14/cr-cdef/12-13/c1213056.asp.

Avis n°5-2013 du Conseil national du numérique sur les libertés numériques. Paris: Conseil national du numérique, Dec. 6, 2013. Available at: http://www.cnnumerique.fr/libertes-numeriques/.

Bas, Philippe. *Rapport de la commission des Lois sur le projet de loi relatif au renseignement*. 460. Sénat, May 20, 2015. Available at: http://www.senat.fr/rap/l14-460/l14-460.html.

Bigo, Didier et al. *National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*. Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs PE 509.991. Brussels: European Parliament, 2014, p. 156. Available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282014%29509991.

Boulaud, Didier. *Avis n°94 sur le projet de loi de finances pour 2008 (Défense - Environnement et soutien de la politique de défense)*. Paris: Sénat, Nov. 22, 2007. Available at: http://www.senat.fr/rap/a07-094-7/a07-094-74.html.

Caeneuve, Bernard. *Réponse du ministre de l'Intérieur à l'avis de la Commission Nationale Consultative des Droits de l'Homme relatif au projet de loi sur le renseignement*. Paris: Ministère de l'Intérieur, Apr. 24,

2015, p. 14. Available at: http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Avis-de-la-CNCDH-sur-le-projet-de-loi-sur-le-renseignement.

Concluding observations on the fifth periodic report of France. CCPR/C/FRA/CO/5. Geneva: Human Rights Committee of the United Nations, July 21, 2015. Available at: https://archive.is/dUrgw.

Gouvernement. *Étude d'impact du projet de loi n° 2669 relatif au renseignement*. République française, Mar. 18, 2015. Available at: http://www.assemblee-nationale.fr/14/projets/pl2669-ei.asp#P432_56763.

Griesbeck, Nathalie et al. *Written question - French Government bill on intelligence*. E-005968/2015. European Parliament, Apr. 15, 2015. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2015-005968+0+DOC+XML+V0//EN.

La Rue, Frank. *2013 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Geneva: United Nations Human Rights Council, Apr. 2013. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Laurent, Sébastien-Yves. *Pour une véritable politique publique du renseignement*. Paris: Institut Montaigne, 2014, p. 96. Available at: http://www.institutmontaigne.org/fr/publications/pour-une-veritable-politique-publique-du-renseignement.

Les Français et la protection de la vie privée. Paris: Institut CSA pour Ordre des Avocats de Paris, July 2015, p. 19. Available at: http://www.csa.eu/multimedia/data/etudes/etudes/etu20150715-Sondage-Francais-Protection-Vie-privee.pdf.

Livre blanc sur la Défense et la Sécurité nationale. Paris: Gouvernement français, June 2008.

Projet de loi relatif à la sécurité et à la lutte contre le terrorisme - Analyse. Ligue des droits de l'Homme, Oct. 5, 2012. Available at: http://www.ldh-france.org/IMG/pdf/analyse_du_projet_de_loi.pdf.

Raffarin, Jean-Pierre. *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*. Paris: Parlement français, Feb. 25, 2016. Available at: http://www.assemblee-nationale.fr/14/rap-off/i3524.asp.

Richard, Jacky and Laurent Cytermann. *Le numérique et les droits fondamentaux*. Les rapports du Conseil d'État. Conseil d'État, Sept. 9,

2014. Available at: http://www.ladocumentationfrancaise.fr/rapports-publics/144000541/index.shtml.

T-CY Guidance Note #3 Transborder access to data (Article 32). T-CY (2013)7 E. Strasbourg: Council of Europe, Dec. 3, 2014. Available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V11.pdf.

The Amesys Case. Paris: FIDH, Feb. 11, 2015. Available at: https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf.

The Global Principles on National Security and the Right to Information (Tshwane Principles). Open Justice Initiative, June 12, 2013. Available at: https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

Urvoas, Jean-Jacques. *Rapport de la commission des Lois sur le projet de loi relatif au renseignement*. Assemblée nationale, Apr. 2, 2015. Available at: http://www.assemblee-nationale.fr/14/rapports/r2697.asp.

— *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*. 2482. Assemblée nationale, Dec. 18, 2014. Available at: http://www.assemblee-nationale.fr/14/rap-off/i2482.asp.

Urvoas, Jean-Jacques and Floran Vadillo. *Réformer les services de renseignement français*. Paris: Fondation Jean Jaurès, May 2, 2011, p. 44. Available at: http://www.jean-jaures.org/Publications/Essais/Reformer-les-services-de-renseignement-francais.

Urvoas, Jean-Jacques and Patrice Verchère. *Rapport en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*. Commission des Lois 1022. Paris: Assemblée nationale, May 14, 2013. Available at: http://www.assemblee-nationale.fr/14/controle/lois/renseignement.asp.

Vadillo, Floran. *Une loi relative aux services de renseignement : l'utopie d'une démocratie adulte ?* Paris: Fondation Jean Jaurès, Apr. 18, 2012. Available at: http://www.jean-jaures.org/Publications/Notes/Une-loi-relative-aux-services-de-renseignement-l-utopie-d-une-democratie-adulte.

Wetzling, Thorsten. *The Key to Intelligence Reform in Germany*. stiftung neue verantwortung, Mar. 2, 2016. Available at: http://www.stiftung-nv.de/publikation/key-intelligence-reform-germany.

Éléments d'analyse technique du projet de loi relatif au renseignement. INRIA, Apr. 30, 2015. Available at: http://sciences.blogs.liberation.fr/files/265206918-note-interne-de-l-inria.pdf.

News articles

Affaire des fadettes : Squarcini condamné à 8000 euros d'amende. Mediapart. Apr. 8, 2014. Available at: https://www.mediapart.fr/journal/france/080414/affaire-des-fadettes-squarcini-condamne-8000-euros-damende.

Alonso, Pierre and Willy Le Devin. *Francis Delon trop près de ses sources*. Sept. 15, 2015. Available at: http://www.liberation.fr/france/2015/09/15/francis-delon-trop-pres-de-ses-sources_1383279.

Baumgärtner, Maik et al. *Spying Close to Home: German Intelligence Under Fire for NSA Cooperation*. Apr. 24, 2015. Available at: http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html.

Borredon, Laurent. *La liste musclée des envies des policiers*. Dec. 5, 2015. Available at: http://www.lemonde.fr/attaques-a-paris/article/2015/12/05/la-liste-musclee-des-envies-des-policiers_4825245_4809495.html.

Bowcott, Owen and Richard Norton-Taylor. *UK spy agencies have collected bulk personal data since 1990s, files show*. Apr. 21, 2016. Available at: http://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s.

Burgess, Matt. *Investigatory Power Bill: UN warns UK's plans 'undermine' the right to privacy*. Wired UK. Mar. 9, 2016. Available at: http://www.wired.co.uk/news/archive/2016-03/09/un-privacy-ip-bill-not-compliant-international-law.

Champeau, Guillaume. *Loi Renseignement : des sondes directement chez les FAI et hébergeurs*. Numerama. Mar. 10, 2015. Available at: http://www.numerama.com/magazine/33120-loi-renseignement-des-sondes-directement-chez-les-fai-et-hebergeurs.html.

Chapuis, Nicolas. *Urvoas : "Je n'ai pas rencontré de programme de surveillance similaire en France"*. June 12, 2013. Available at: http://www.lemonde.fr/politique/article/2013/06/12/urvoas-je-n-ai-pas-rencontre-de-programme-de-surveillance-similaire-en-france_3428507_823448.html.

De Safari à Edvige : 35 années d´une Histoire oubliée malgré la création de la CNIL. Mag-Securs. Feb. 8, 2009. Available at: http://www.mag-securs.com/news/articletype/articleview/articleid/23700/de-safari-a-edvige--35-annees-d8217une-histoire-oubliee-malgre-la-creation-de-la-cnil.aspx.

Deléan, Michel and Louise Fessard. *L'antiterrorisme est à la peine depuis 2008*. Mediapart. Nov. 14, 2015. Available at: https://www.mediapart.fr/journal/france/141115/l-antiterrorisme-est-la-peine-depuis-2008?onglet=full.

Dutch govt approves new wiretapping legislation. Telecompaper. Apr. 18, 2016. Available at: http://www.telecompaper.com/news/dutch-govt-approves-new-wiretapping-legislation--1138892.

Déléan, Michel. *Un ex-directeur de la DGSE: «On a baissé la garde sur le renseignement humain»*. Mediapart. Nov. 20, 2015. Available at: https://www.mediapart.fr/journal/france/201115/un-ex-directeur-de-la-dgse-baisse-la-garde-sur-le-renseignement-humain?onglet=full.

Follorou, Jacques. *Comment la DGSE a pu espionner des Français*. May 2016. Available at: http://www.lemonde.fr/societe/article/2016/04/13/comment-la-dgse-a-pu-espionner-des-francais_4901155_3224.html.

— *Comment la DGSE a surveillé Thierry Solère*. Apr. 12, 2016. Available at: http://www.lemonde.fr/societe/article/2016/04/12/comment-la-dgse-a-surveille-thierry-solere_4900451_3224.html.

— *Le renforcement du contrôle se heurte à la coopération internationale entre services*. Aug. 22, 2013. Available at: http://www.lemonde.fr/societe/article/2013/08/22/le-renforcement-du-controle-se-heurte-a-la-cooperation-internationale-entre-services_3464714_3224.html.

— *Les failles de la lutte antiterroriste*. Nov. 20, 2015. Available at: http://www.lemonde.fr/attaques-a-paris/article/2015/11/19/les-failles-de-la-lutte-antiterroriste_4813166_4809495.html.

— *Renseignement : histoire d'une révolution avortée*. Feb. 5, 2016. Available at: http://www.lemonde.fr/police-justice/article/2016/02/04/renseignement-histoire-d-une-revolution-avortee_4859309_1653578.html.

— *Surveillance : la DGSE a transmis des données à la NSA américaine*. Le Monde.fr. Oct. 30, 2013. Available at: http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.

Follorou, Jacques. *Tensions autour du contrôle du renseignement*. Le Monde. Mar. 5, 2016. Available at: http://www.lemonde.fr/societe/article/2016/03/05/tensions-autour-du-controle-du-renseignement_4877127_3224.html.

Follorou, Jacques and Franck Johannès. *La totalité de nos communications espionnées par un supercalculateur*. July 4, 2013. Available at: http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.

Fradin, Andréa. *Le surveillant des espions « a rendu des avis nuit et jour »*. Rue89. Nov. 18, 2015. Available at: http://rue89.nouvelobs.com/2015/11/18/surveillant-espions-a-rendu-avis-nuit-jour-262170.

— *Loi renseignement : l'Assemblée décommande Blue Coat, dont les machines fliquent le Web syrien*. Rue89. Mar. 25, 2015. Available at: http://rue89.nouvelobs.com/2015/03/25/loi-renseignement-lassemblee-decommande-blue-coat-dont-les-machines-fliquent-web-syrien-258376.

Hourdeaux, Jérôme. *Comment les services de renseignement ont mis en place une surveillance générale du Net dès 2009*. Mediapart. June 6, 2016. Available at: https://www.mediapart.fr/journal/france/060616/comment-les-services-de-renseignement-ont-mis-en-place-une-surveillance-generale-du-net-des-2009.

— *Surveillance: la justice enquête sur les liens entre Qosmos et la Syrie*. Mediapart. Apr. 11, 2014. Available at: https://www.mediapart.fr/journal/international/110414/surveillance-la-justice-enquete-sur-les-liens-entre-qosmos-et-la-syrie.

Hourdeaux, Jérôme, Bluetouff, and Kitetoa. *Qosmos : du projet universitaire aux activités "secret-défense"*. Mediapart. May 7, 2014. Available at: https://www.mediapart.fr/journal/international/070514/qosmos-du-projet-universitaire-aux-activites-secret-defense.

Jauvert, Vincent. *Comment la France écoute (aussi) le monde*. L'Obs. July 1, 2015. Available at: http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html.

— *Le DGSE écoute le monde (et les Français) depuis plus de trente ans*. NouvelObs.com. July 4, 2013. Available at: http://globe.blogs.nouvelobs.com/archive/2013/07/04/comment-la-france-ecoute-le-monde.html.

Johannès, Franck. *Renseignement : l'amendement de dernière minute qui embarrasse le gouvernement*. Le Monde.fr. June 20, 2015. Available at: /societe/article/2015/06/20/renseignement-le-cas-a-part-des-etrangers_4658456_3224.html.

Johannès, Franck and Simon Piel. *"Kairos", le lien public-privé du renseignement français*. Le Monde.fr. Oct. 28, 2013. Available at: http://www.lemonde.fr/societe/article/2013/10/28/qosmos-collabore-avec-le-renseignement-francais_3503940_3224.html.

kitetoa. *Palantir et la France : naissance d'une nouvelle théorie abracadabrantesque ?* Nov. 19, 2015. Available at: https://reflets.info/palantir-et-la-france-naissance-dune-nouvelle-theorie-abracadabrantesque/.

Le FSI épaule les grandes oreilles. Intelligence Online. Sept. 29, 2011. Available at: http://www.intelligenceonline.fr/intelligence-economique/2011/09/29/le-fsi-epaule-les-grandes-oreilles,93184212-ART-HOM.

Lettre ouverte aux membres du Conseil constitutionnel. July 20, 2015. Available at: https://blogs.mediapart.fr/edition/les-invites-de-mediapart/article/200715/lettre-ouverte-aux-membres-du-conseil-constitutionnel.

Loi sur le renseignement: François Hollande va saisir le Conseil constitutionnel. L'Express. Apr. 19, 2015. Available at: http://www.lexpress.fr/actualite/politique/loi-sur-le-renseignement-hollande-va-saisir-le-conseil-constitutionnel_1672751.html.

Manach, Jean Marc. *Frenchelon: la DGSE est en « 1ère division »*. BUG BROTHER. Oct. 2, 2010. Available at: http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division/.

— *La DGSE a le « droit » d'espionner ton Wi-Fi, ton GSM et ton GPS aussi*. BUG BROTHER. July 11, 2013. Available at: http://www.lemonde.fr/iframe/jelec.html.

Marc Trévidic dénonce les dérives de la loi sur le renseignement. RTL.fr. Apr. 7, 2015. Available at: http://www.rtl.fr/actu/societe-faits-divers/la-loi-sur-le-renseignement-entre-de-mauvaises-mains-est-une-arme-redoutable-estime-le-juge-marc-trevidic-7777296541.

Muižnieks, Nils. *Lettre du Commissaire aux droits de l'homme du Conseil de l'Europe aux membres de la Commission des lois du Sénat français sur le projet de loi relatif au renseignement*. May 18, 2015. Available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH(2015)13&Language=lanFrench.

Rees, Marc. *Deux députés s'attaquent au chiffrement*. Mar. 1, 2016. Available at: http://www.nextinpact.com/news/98821-deux-deputes-sattaquent-au-chiffrement.htm.

Rees, Marc. *Loi Renseignement : l'avis que la CNIL refuse de publier*. Feb. 10, 2016. Available at: http://www.nextinpact.com/news/98483-loi-renseignement-avis-que-cnil-refuse-publier.htm.

Reflets.info. *Qosmos et le gouvernement Français, très à l'écoute du Net dès 2009*. Reflets. June 6, 2016. Available at: https://reflets.info/qosmos-et-le-gouvernement-francais-tres-a-lecoute-du-net-des-2009/.

Szary, Wiktor. *Poles rally against new surveillance law amid 'Orbanisation' fears*. Jan. 23, 2016. Available at: http://www.reuters.com/article/us-poland-protests-idUSKCN0V10JV.

The Editorial Board. *The French Surveillance State*. Mar. 31, 2015. Available at: http://www.nytimes.com/2015/04/01/opinion/the-french-surveillance-state.html.

Urvoas, Jean-Jacques. *Big Brother à la française ? Commentaires*. Le blog de Jean-Jacques Urvoas. July 4, 2013. Available at: http://archive.is/7SGgk.