Internet Surveillance in France's Intelligence Act

Félix Tréguer

Internet Surveillance in France's Intelligence Act

Félix Tréguer*
felix.treguer@sciencespo.fr

October 2016

Abstract

This brief offers an overview of France's Intelligence Act of July 2015, and in particular of its provisions surrounding Internet surveillance.

The Intelligence Act of 24 July 2015 (*loi relative au renseignement*) is a statute passed by the French Parliament. The law created a new chapter in the Code of Internal Security aimed at regulating the surveillance programs of French intelligence agencies, in particular those of the DGSI (domestic intelligence) and the DGSE (foreign intelligence).

Background

The Intelligence Bill was introduced to the Parliament on 19 March 2015 by French Prime Minister Manuel Valls (Socialist Party) and presented as the government's reaction to the Charlie Hebdo shooting. Despite widespread mobilization, 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. It was made into law on 24 July 2015.

Although framed by the government as a response to the Paris attacks of January 2015, the passage of the Intelligence Act was actually long in the making. The previous law providing a framework for the surveillance programs of French intelligence agencies was the Wiretapping Act of 1991,

*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.

aimed at regulating telephone wiretaps. Many surveillance programs developed in the 2000s –especially to monitor Internet communications—were rolled out outside of any legal framework. As early as 2008, the French government's White Paper of Defense and National Security stressed that "intelligence activities do not have the benefit of a clear and sufficient legal framework", and said that "legislative adjustments" were necessary.

General provisions

Compared to the 1991 Wiretapping Act (the previous statute in the field of secret sate surveillance), the 2015 Intelligence Act enacts an unprecedented extension of the scope of so-called "intelligence-gathering techniques." Through article L. 811-3,[1] 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.

The government is allowed to extend by decree the number of law enforcement agencies who may conduct extra-judicial surveillance.[2] 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).

[1] Unless stated otherwise, all articles mentioned here are part of the Code of Internal Security.

[2] 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.

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;[3]
- 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 previous 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 authorizations delivered by the Prime Minister before surveillance begins,[4] 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

[3]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.

[4]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.

foreign partners is likely to contain data on French residents, appears to be a pressing request from intelligence officials.[5]

Wiretaps and access to metadata

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.

Black boxes and real-time access to metadata

The Act authorizes the use of scanning device (nicknamed "black boxes") to be installed on the infrastructures of telecom operators and hosting providers. 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.[6]

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

[5] 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.

[6] 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.*"

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.[7]. 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.[8] 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.[9] 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. 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”–[10] remains dubious.

Another provision limited to anti-terrorism allows for the real-time collection of metadata (article L. 851-3, for terrorism only and for a 4 months period). Initially, the provision targeted only individuals “identified as a [terrorist] threat.” After the 2016 Nice Attack, it was extended by a Bill of the state of emergency to cover individuals “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.”

[7]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).

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

[9]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.

[10]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.

Computer Network Exploitation

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

- 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.[11]

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

[11] 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.

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.

- 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 21st 2016.[12]

[12]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/.

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).

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.[13]

Moreover, international surveillance remains outside of the scope of the redress procedure, as was confirmed by a ruling of the Constitutional Council,[14], 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.[15]

[13]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.

[14]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.*"

[15]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.

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.[16]

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