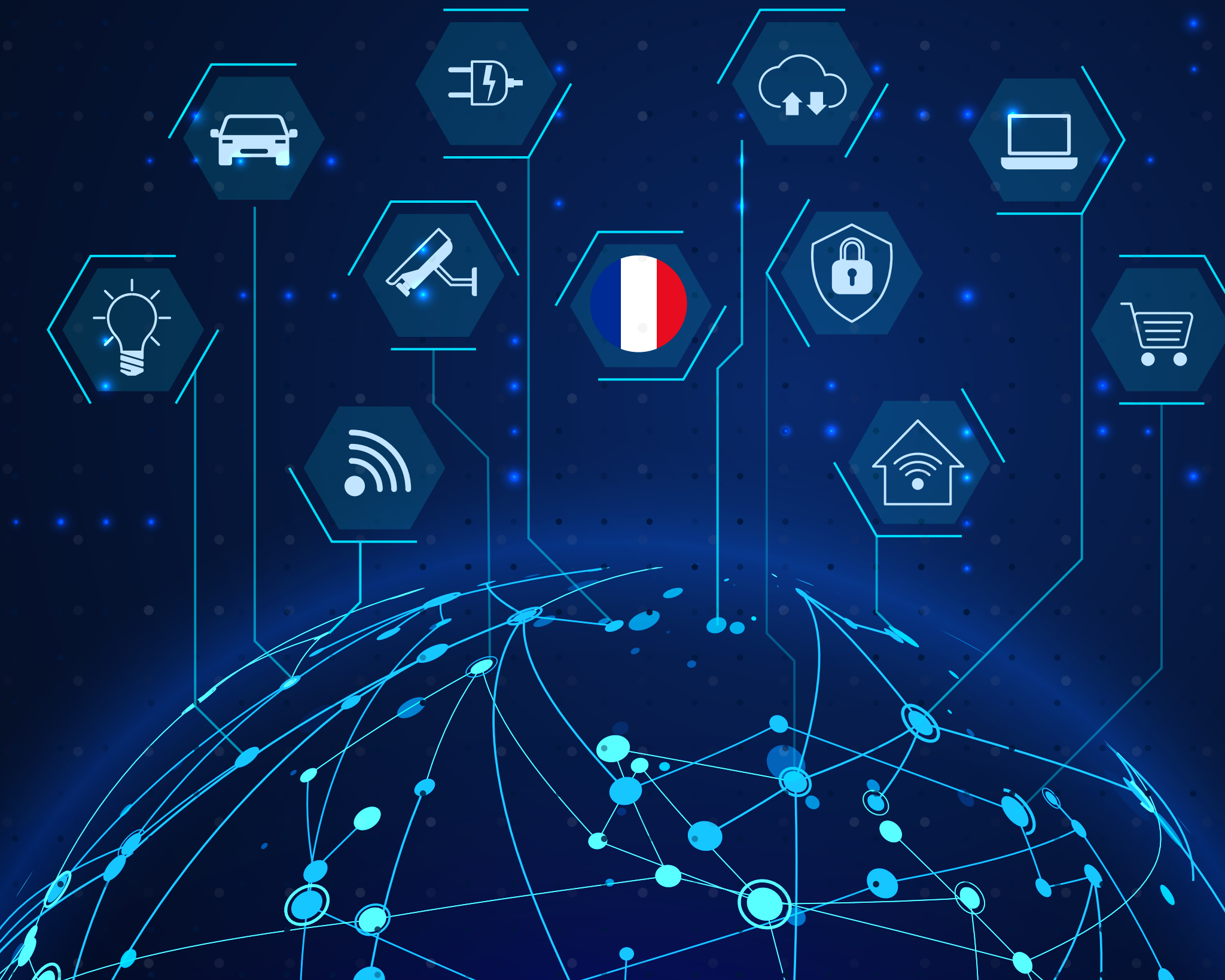
SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

SURVEILLANCE NORMS:
TOWARD A BASELINE CONSENSUS AMONG DEMOCRATIC STATES

COMMUNICATION SURVEILLANCE IN FRANCE

Sébastien-Yves Laurent



ABOUT THE AUTHOR

Pr. Dr Sébastien-Yves Laurent, a political scientist and an historian is a tenured Professor (Fac. of Law and Political Science) at the University of Bordeaux. He published widely in the field of "Security Studies" in several Journals and has published several books and edited collections (last published: Conflicts, Crimes and Regulations in Cyberspace, Wiley, 2021).

ACKNOWLEDGEMENTS

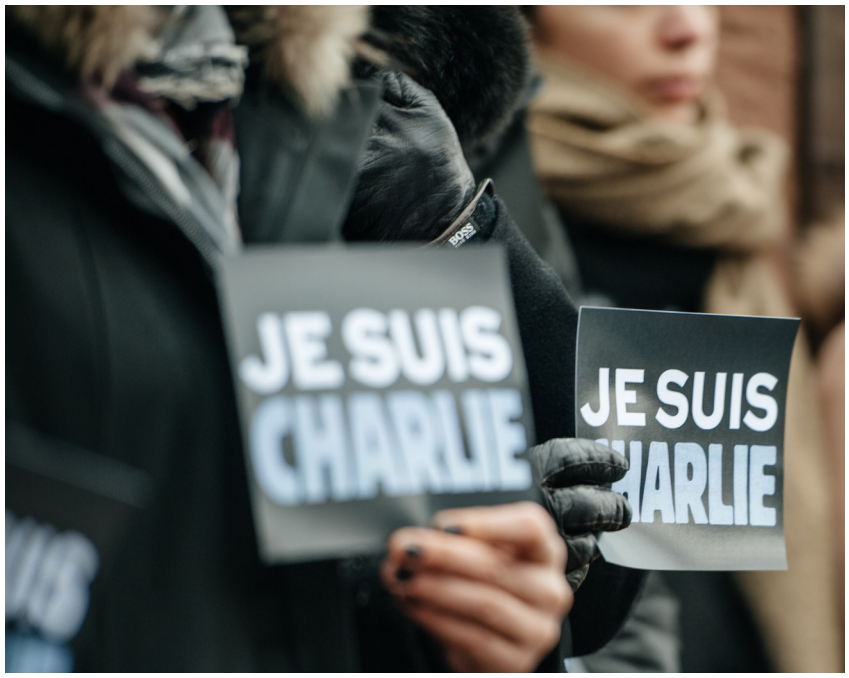
This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

I. INTRODUCTION

Since the enactment of a new Act in July 2015 – in the wake of terror attack of January 2015 in Paris (hereafter "Charlie Hebdo terror attack") – France has erected a new legal and technical framework for surveillance. However, the current framework is the result of a long process of legal, policy, and institutional sedimentation which began in 1960.



I.1. Before 1991, the police and the intelligence services had considerable discretion to conduct telephone wiretapping. It hinged on customary and shadowy practices. This first structuring of domestic surveillance (before 1991) was set up in 1960 during the so-called Algerian War, relying only on a non-public written act.[1] The keystone of this first structuring was the written authorization by the Prime Minister's Office for each tapping.[2] Even after the war ended in 1962, domestic security surveillance remained in the hands of the Executive Branch, without accountability and oversight.

Predictably, the system was misused, including for political purposes. Throughout the Fourth and Fifth Republics, there has been a latent feeling that political opponents were regularly tapped by the administration (i.e., by the political majority). At the beginning of the seventies, the issue was obliquely raised at the Assembly by the political opposition. Despite an implicit acceptance, this practice fueled distrust towards police and intelligence services among politicians and the public. For the first time, in June 1973, an inquiry committee was set up in the Senate. Despite efforts by the administration to obstruct the inquiry, the resulting report clearly established the structural use of phone tapping by the governments.[3] The report was made public in November 1973. Despite this, tapping remained utterly unchained. Until 1991, it led to bitter recriminations throughout the life of the Fifth Republic (the present constitutional order, which began in 1958), even if secrecy made it impossible to accurately assess the scale of the problem.

I.2. The second legal era of domestic surveillance began in 1991, after the European Court of Human Rights (ECHR) held that the status quo contravened the European Convention on Human Rights. Specifically, in April 1990, two unanimous ECHR judgements, *Huvig* and *Kruslin*, condemned France for the lack

of solid written rules with regard to phone tapping in judicial inquiries.[4] In the wake of those decisions, the French Government, headed by Prime Minister Michel Rocard, anticipated that phone tapping requested by intelligence services would be the next concern for the ECHR (as had happened against UK in 1984 with the *Malone* judgment), so it sought legislation to pre-empt such a judgment.

> ***The Act that passed in 1991 created a new legal framework, which laid the foundation of the current system.***

The Act that passed in 1991 created a new legal framework, which laid the foundation of the current system. Among its innovations was a dedicated committee, the "Commission nationale de contrôle des interceptions de sécurité" (CNCIS). Indeed, the new legislation enacted after the Charlie Hebdo terror attack in July 2015 (2015-912 Act) largely left the post-1991 system in place, with changes to reflect new technologies and reinforce external oversight. At that time, it appeared that France imposed the most demanding technical and procedural standards in Western late democracies.

The 1991 Act is thus a milestone in the French legal and technical framework dedicated to surveillance. It made public the shadowy process created in 1960 and it set up foundational principles, including the authorization process and oversight mechanisms.

Most importantly, the operational entity that executed phone tapping (the "Groupement interministériel de contrôle," (GIC), created in 1960), which was subordinate to the Prime Minister's Office,[5] was made public for the first time.[6] One effect of this was to reveal the prominent role played by the Prime Minister's office in conducting surveillance. For the first time, an Act which had been the subject of a public debate in Parliament confirmed the direct role of the Executive Branch.

A second major change involved *authorization* for phone taps: Prime Ministerial authorization, in place since the "Algerian War," was replaced by a new independent body, the "Commission nationale de contrôle des interceptions de sécurité" (CNCIS). In theory, according to the provisions of the Act, the Committee was an advisory structure, but as soon as it began to work, the Prime Minister's Office began to systematically follow its advice. It is an indication of the liberal evolution of the Executive Branch with regard to practices that until then had been within its "reserved domain."[7]

The Act also introduced new statutory categories: "interceptions de sécurité," i.e., phone tapping, hereafter referred to as "security intercepts." Importantly, "security intercepts" also included metadata (referred to as "connection data"). The CNCIS Committee exercised a twofold control on security intercepts: a priori (pre-approval) and a posteriori (post hoc) (detailed below in Section II). The Intelligence services had to ground each request in one of the five purposes mentioned in the Act: (1) "national security," (2) "safeguarding the essential elements of France's scientific and economic potential,"[8] (3) "prevention against terrorism," (4) "fight against organized crime," and (5) "fight against armed militias." Surveillance for political purposes was excluded. The CNCIS would then check that the request was plausible and that it complied with the specified purpose. The CNCIS was composed of Judges and Parliamentarians, appointed by heads of the main juridical bodies and by the two assemblies. In the French juridical tradition, the CNCIS is considered to have jurisdiction, even if its jurisdiction is a very peculiar one.[9] Each year, it submits a public report comprising an activity report, figures on security intercepts (including detailed figures related to the five purposes), comments on post hoc control, remarks on the way the intelligence services complied with the 1991 Act, and even proposals for the evolution of the legal framework.

I.3. The last and current legal framework for domestic surveillance dates to 2015 and the Charlie Hebdo terror attack. The July 2015 Act (2015-912 Act) left much in place while establishing some new concepts and practices. The body in charge of undertaking phone tapping and electronic surveillance, the GIC, remained unchanged. So did the authorization process, which remains entrusted to a committee (even if from a legal point of view the Prime Minister's Office delivers the authorization, *see* Section I.2, *supra*).

The main novelty of the 2015 Act lies in new

denominations and in new legal capabilities to undertake surveillance measures. Most notably, the 1991 Act's "security intercepts" (*see* Section I.2, *supra*) were replaced by "intelligence techniques," a far more precise notion encompassing a broader range of operational methods (*see* Section III, *infra*). Moreover, the new Act revised threats/motives, allowing the Intelligence agencies to make requests for surveillance (*see* Section III, *infra*). Lastly, the Act replaced the CNCIS Committee with a new body, the CNCTR Committee, with broader oversight powers (*see* Section II, *infra*).

II. INSTITUTIONS

Operational Entities

Domestic surveillance (phone tapping originally, then electronic surveillance) has been implemented by the same unit, the "Groupement interministériel de contrôle" (GIC), since its inception in 1960. This unit was (and remains) subordinate to the Prime Minister's cabinet office. Set up during the Algerian War, it has always been headed by a military officer of flag-officer rank. Despite this, it is a civilian entity whose workforce (around 250 people) is composed mainly of civilians, police officers, and translators. Situated in Paris, the GIC has sub-units across French territory (including overseas). The GIC interacts directly with telephone operators and with Internet providers, and is empowered by law to obtain data and metadata directly from them. The GIC reports only to the Prime Minister and was initially overseen by the CNCIS (from 1991 to 2015), and then by the CNCTR (from 2015 on) (see below).

The GIC is not allowed to undertake technical intelligence activities (i.e., phone tapping) on its own. Its responsibility is limited to *implementing* interception requested by the intelligence agencies and authorized by the CNCTR committee. The former 1991 Act and the current 2015 Act allow only the Intelligence Agencies to make request for surveillance. Currently, six intelligence agencies are allowed to make requests: the Direction générale de la sécurité extérieure (DGSE), the Direction générale de la sécurité intérieure (DGSI), Direction du renseignement militaire (DRM), the Direction du renseignement et de la sécurité de défense (DRSD), the Direction nationale des enquêtes douanières (DNRED-customs), and the Traitement du renseignement et action contre les circuits financiers clandestins (Tracfin-financial intelligence unit).

1) The DGSE is France's only foreign-intelligence agency, and it reports to the Président de la République (though it is attached to the Ministry of Defense). The workforce is roughly 75% civilian, 25% military.

2) The DGSI is responsible for domestic security intelligence (i.e., counter-espionage, counter-terrorism, and counter-interference) and it reports to the Home Office ("ministère de l'Intérieur"). Until 2022, the workforce was almost exclusively composed of police officers.

3) The DRM is the main defense intelligence agency. It reports to the chief of staff ("chef d'état-major des armées") and is attached to the Ministry of Defense.

4) The DRSD is a military intelligence agency specialized on military security intelligence. It is tasked with protecting military units and administration (but also private military industries) against foreign interference.

5) The DNRED attached to the Ministry of Economics and Finance is in charge of the fight against organized crime.

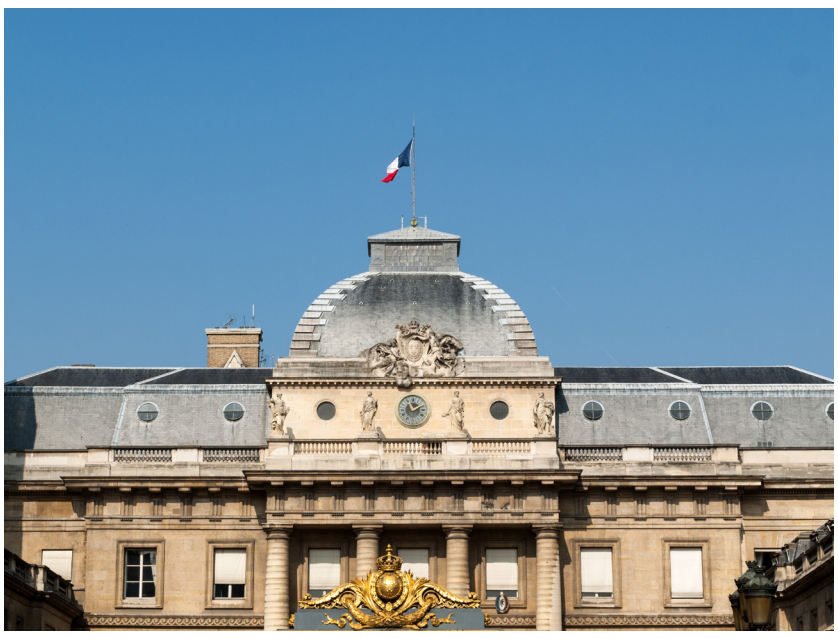
6) TRACFIN is the French financial intelligence unit, attached to the Ministry of Economics and Finance.

None of the six agencies is allowed to undertake technical domestic surveillance without the GIC. Each agency has its own technical capabilities but for other purposes than those mentioned in the 1991 and 2015 Acts. The DGSE is separate: it is responsible for conducting international surveillance, and since the 2000s, this mission has been executed by its "direction technique" (one of the five main directorates within the DGSE). Bulk access operations are undertaken abroad by the DGSE without being subject to a written legal framework.

Authorizing and Oversight Entities

The CNCTR ("Commission nationale de contrôle des techniques de renseignement") was created in 2015 and succeeded the CNCIS (*see* section 2). The CNCTR is central to the French way of authorizing and overseeing national security surveillance. Like the CNCIS, the

CNCTR is an "autorité administrative indépendante," i.e., a jurisdiction (*see* footnote 8, *supra*). Before being implemented by the GIC, the "intelligence techniques" (as mentioned in the 2015 Act, *see* sections I.3 and III) must be pre-approved by the CNCTR. The Committee checks that the request made by an intelligence agency complies with the purposes listed in the Act. Moreover, it examines whether the request respects the proportionality and the subsidiarity principles in answering this kind of query: are there any other means of inquiry, less intrusive, that could lead to the same result? Then, once the technique has been implemented, the Committee exercises its a posteriori (post hoc) control. It checks that the implementation occurred in the manner specified by the Act. To this end, it has access to the transcripts or results of the techniques and can proceed to on-site inspections. The CNCTR is composed of nine members: four parliamentarians, four judges, and one "qualified person."[10]



The 2015 Act has introduced a new right of appeal for individuals. They can make a request to the CNCTR to check whether they have been subject to an unlawful surveillance technique. If the CNCTR finds an unlawful technique, it can ask the Prime Minister to stop it and to destroy/delete the result. Plaintiffs do not learn whether or not they have been surveilled. The 2015 Act also introduced a second instance for an appeal, the Conseil d'Etat, which is in French Law an actual judicial organ (this is the highest administrative jurisdiction, *see* footnote 8) and not a simple Committee, as the CNCTR is.

Legislative oversight is provided by a select parliamentary committee, the so-called "délégation parlementaire au renseignement," or DPR. The DPR, which was created in 2007, oversees the CNCTR and the intelligence agencies, but does not directly review individual instances of surveillance carried out by the agencies. However, it should be recalled that four members of Parliament are appointed to the CNCTR (out of nine members of that body).

III. OPERATIONAL CAPABILITIES AND PRIORITIES

The arrangement that prevailed between 1991 and 2015 suffered from several weaknesses. On the one hand, it was unclear if the 1991 Act covered over-the-airwaves communication (mobile phones), and therefore there was room for litigation. It never happened, but from 1991 to 2015 the government had to live with this legal uncertainty. The Charlie Hebdo terror attack served as a tragic impetus to resolve this uncomfortable statutory uncertainty. Similarly, in the years after the 1991 law, law enforcement and intelligence services sought to adapt to new digital technologies as they investigated organized crime and terrorism. The problem was that these new techniques were not clearly authorized by the 1991 Act or even by other pieces of legislation. Investigations that employed these potentially unauthorized techniques were thus at risk. The practical consequences of that risk were limited when intelligence services were involved because there was no judicial oversight of their investigations. Nonetheless, as in 1990, the French government feared being held liable by the European Court of Human Rights for using allegedly unlawful intelligence techniques (*see* section I.2).

The government was well of aware of such a risk and had prepared a Bill to expand the agencies' powers to accommodate new and emerging technologies. The Charlie Hebdo terror attack, which occurred in January 2015, catalyzed those changes. In July 2015, the Parliament passed the 2015-912 Act "relating to Intelligence," the first of its kind in France. Being of such high importance in the context of a terror attack on French soil, the Président de la République himself appealed to the Supreme Court (i.e., the Conseil Constitutionnel), a very rare way to proceed. The Conseil Constitutionnel, by the 2015-713 decision (2015, July 23), validated the heart of the Bill and invalidated minor aspects (*see* Section IV, *infra*).

This Act precisely defined all technical methods that can be requested by the intelligence services, referred to as "techniques de renseignement" (hereafter "intelligence techniques") in the new Act. The list mentioned nine "intelligence techniques": (1) connection data (i.e., metadata) in real and delayed time, (2) detection algorithms applied to communication,[11] (3) geolocation of persons and objects, (4) location of persons and objects by beacon, (5) IMSI catchers, (6) security intercepts (content telephone tapping), (7) speech capture (bugging a room), (8) image capture (filming a room), and (9) computer data capture (by using malware). All these intelligence techniques must be used only on individual targets. There is no room for bulk access under this piece of legislation.

> ***The passage of the new Act on the "techniques de renseignement" is major development in surveillance law in France. It represents an unprecedented enlargement and legalization of the means at the disposal of the intelligence services.***

The passage of the new Act on the "techniques de renseignement" is major development in surveillance law in France. It represents an unprecedented enlargement and legalization of the means at the disposal of the intelligence services. From 2015 on, they have had the ability to use a wide array of means that were before the exclusive province of the law enforcement services. Despite the context of terror attacks (January and November 2015), some non-governmental organizations (NGOs) (French Data Network, Quadrature du Net, journalists, barristers) mobilized and appealed against the Act in France and in the European Union (*see* Section V, *infra*).

The 2015-912 Act also added to and modified the five purposes for security intercepts specified in the 1991 law (*see* Section I.2, *supra*). The new or modified purposes included: "national independence, territorial integrity and national defense," "France's major economic, industrial and scientific interests," and "preventing the proliferation of weapons of mass

destruction." In practice, the seven broadly defined purposes in the new Act gave intelligence agencies wide latitude to make requests for surveillance. This heightens the importance of the CNCTR committee's review to make sure that the proportionality principle is observed.

There is no open-source material on the technical sophistication of the GIC. One can only make the hypothesis that it benefits from the high technological levels of the "direction technique" of the Direction générale de la sécurité extérieure (DGSE) (see Section II, supra) and from the Agence nationale de la sécurité des systèmes d'information (ANSSI), the national cybersecurity agency. Insofar as there is no independent technical agency for SIGINT collection as in most countries, it falls within the responsibility of the DGSE. One can assume that the best technological abilities are located in the DGSE. Even if the DGSE is not at all involved in domestic surveillance, it may perhaps share its technical experience with other French agencies. One should also recall that in June 2022, Gina Haspel, who headed the CIA from 2018 to 2022, declared publicly that the DGSE was in the "top three" intelligence agencies,[12] a judgment that could not have been made without taking into account the DGSE's technical capabilities.

In 2011, the French government disclosed[13] that one year ago, one dedicated committee at the French presidency (the "Coordination nationale du renseignement et de la lute contre le terrorisme," CNRLT) was tasked with establishing a "National Intelligence orientation plan" ("Plan national d'orientation du renseignement," PNOR). The plan establishes the intelligence services' collection priorities and is revised each year. Despite not being public, the PNOR is subject to parliamentary oversight. Nevertheless, currently in the French political culture surveillance cannot be an intelligence aim *per se* (even if it obvious that bulk collection abroad is a necessary way to reach other intelligence aims). Lastly, individual surveillance in France doesn't come under 'bulk access' practices: people being the targets of surveillance measures are only individuals and actually very few in number (*see* Section VI, *infra*).

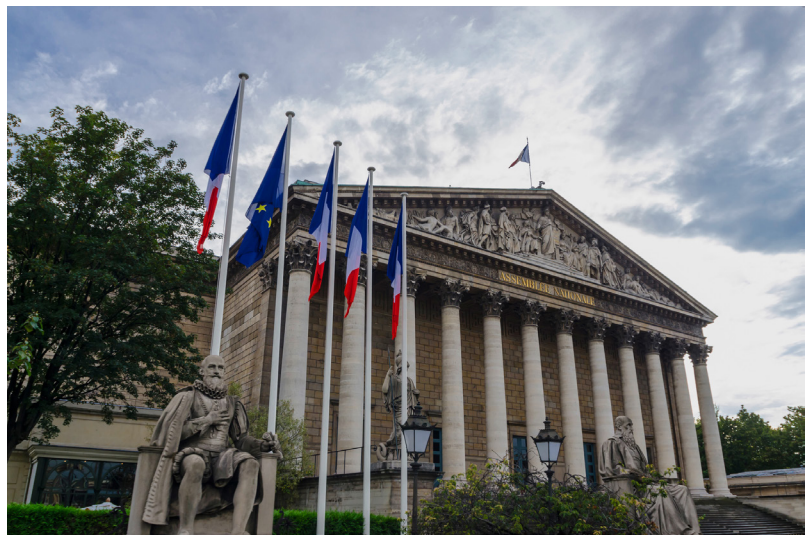
IV. PROCESS FOR CONDUCTING SURVEILLANCE

The basic process for conducting surveillance inside France is set forth by statute and does not differ based on whether the target is a citizen of France or another state. First, an agency makes a request to the GIC to use a particular "intelligence technique" permitted by the 2015 Act (*see* Sections I.3 and III, *supra*). The request is then reviewed by the CNCTR, which checks that the request supports one of the five approved purposes for surveillance. The CNCTR also confirms that the request is proportional and is the least intrusive means of achieving the desired result. Then, once the technique has been implemented, the CNCTR conducts post hoc control to ensure that the surveillance was implemented in the approved, lawful manner.

"International communications," however, are not subject to this process. The 2015-912 Act adopted after Charlie Hebdo permitted signals collection outside the country without external oversight. The Conseil Constitutionnel[14] invalidated those provisions shortly thereafter, fearing that they would subject French citizens to surveillance without oversight. Instead, the Conseil Constitutionnel took the view that the surveillance of French citizens should be systematically overseen, regardless of their location.

Parliament quickly passed another law, the 2015-1556 Act, to replace the invalidated provisions. The new law instead referred to "international communications," for which the Prime Minister's office would approve surveillance without external oversight from the CNCTR.

In a jurisdictional oddity, France's highest juridical bodies both weighed in on the new law. The Conseil Constitutionnel upheld the new language.[15] Then, in 2018, the Conseil d'État weighed in. It construed "international communications" to refer to a foreign country where an individual had subscribed for mobile phone services or where the "technical identifier" (i.e., the selector) used for the collection was assigned.[16] Thus, in the Conseil d'État's view, "international" did not refer to the country where the service is used (i.e., it could be used in France) nor the nationality (and thus it could be used by a French citizen). This lenient interpretation may reflect that the Conseil d'État is customarily sympathetic to the Executive Branch, producing a different approach from the Conseil Constitutionnel with regard to the legal protection of French citizens toward electronic surveillance.



The end result is that the strict process of the 2015-912 Act—agency, GIC, CNCTR—remains the core process for individual surveillance. For "international communications" surveilled under the 2015-1556 Act, however, the CNCTR does not play any role in the authorization process. Instead, the Prime Minister's office approves the surveillance without external oversight.

V. RELEVANT LAW

The legal framework for national security surveillance in France is concise. The 2015-912 Act "relating to Intelligence" and the 2015-1556 Act "relating to measures for the surveillance of international electronic communications" are two unusually short Acts: the first has 23 articles and the latter has 2 articles. There are only general principles but no more: there is no precise guidance, and the French lawmakers have entrusted to the CNCTR the responsibility of interacting with the Intelligence Services with respect to surveillance. Moreover, the CNCTR reports are also short, and the CNCTR maintains a high level of discretion on the deals it reaches with the Intelligence Services. The paucity of the 2015-1556 Act gives a great deal of latitude to the DGSE in conducting bulk access and also to the Executive Branch when it refers to the authorization process. Unsurprisingly, this shows that bulk access comes under national sovereignty and that it cannot be really constrained.

The paucity of the 2015-1556 Act gives a great deal of latitude to the DGSE in conducting bulk access and also to the Executive Branch when it refers to the authorization process.

The only restriction stems from EU judgments. In 2016, the European Court of Justice (CJEU) issued the "Tele2 Sverige" judgment (confirmed in October 2020, "Privacy International"). It forbade the unlimited storage and retention of metadata that the Intelligence Services required from the providers. From the French Government's point of view, the case isn't closed, however: in April 2021, the Conseil d'Etat[17] stated that the 2016 and 2020 judgments dealt with national security, an issue that is clearly outside of the European Treaties. Accordingly, it took the view that the Intelligence Services could require providers to store metadata, despite the CJEU's decision in *Privacy International*.

VI. TRANSPARENCY

France's transparency regime for intelligence programs relies mainly on public annual reports: those published by the "Délégation parlementaire au renseignement" since 2007, those published by the CNCIS since 1993, and by the CNCTR since 2015. Technical intelligence is only with the CNCIS and CNCTR reports. Beginning in 1993 with the first annual report from the CNCIS,[18] the state has disclosed the annual number of security intercepts. Between 1993 and 2014, the security intercepts amounted to an average of 3,000 per year (at that time it referred only to phone tapping).

After 2015, the CNCTR continued the CNCIS's policy, publishing each year in its official reports figures relating to individual domestic surveillance (i.e., the "techniques de renseignement"). The growth comes from the fact that it includes henceforth more than phone tapping.

One can note that terrorism and organized crime are the two main crimes that justify the bulk of individual surveillance (from around 59% to around 70%, depending on the year). Figures related to other kinds of crimes enshrined in the Act as foreign espionage are not detailed in the reports. It can be assumed that this is for security reasons (*cf.* Section V, *supra*).

Despite the Snowden affair in 2013, French public opinion is not really mobilized by surveillance issues. The 2015 terror attacks (and those that followed) led to a "moral shock" that allowed the government to set up a new legal framework giving the Intelligence Services enlarged access to electronic surveillance techniques. NGOs and hacktivists mobilized and appealed but were defeated at the Conseil Constitutionnel. As in other European countries, they had greater success with EU litigation, which is nowadays the principal way to constrain the government on these issues. Broadly speaking, oversight has been reinforced, but surveillance has also increased.

	2016	2017	2018	2019	2020
Individuals under surveillance	20,360[19]	21,386	22,038	22,210	21,952[20]
As part of anti-terrorism efforts	9,475 (46.5%)	9,157 (42.8%)	8,574 (38.9%)	7,736 (34.8%)	8,786 (40%)
As part of the fight against organized crime	4,969 (24.4%)	5,528 (25.8%)	5,416 (24.6%)	5,639 (25.6%)	5,021 (22.9%)

(Sources: 3rd official report 2018, p. 69; 4th official report 2019, p. 58; 5th official report 2020, p. 45.)

ENDNOTES

1. *Décision n° 1E*, 28 March 1960, signed by the Prime Minister. A "decision" is not in fact a decree; rather, it is a tailored and very rare kind of act in the Executive Branch. The "décision" was classified until 1993. It was published in 1993 in the first public report of the CNCIS (see Section I.2, infra).
2. Historical research is based on archives that demonstrated that at the Prime Minister's Office, the advisor for security or the director of the cabinet was in charge of assessing the requests.
3. *Rapport fait au nom de la Commission de contrôle des services administratifs procédant aux écoutes téléphoniques* [Report on behalf of the Administrative Services Review Board carrying out telephone tapping], n° 30, annexe au procès-verbal de la séance du 25 octobre 1973, p. 115.
4. There were, in fact, provisions in the Criminal Procedure Code regulating the issuance of warrants, but these were deemed insufficient by the ECHR.
5. In France, the Executive Branch has two heads, the Prime Minister and the President of the Republic (who is superior to the Prime Minister).
6. It received a statutory basis later by the decree n° 2002-497, signed on 12 April 2002 by the Prime Minister.
7. The "reserved domain" (le "domaine réservé") is an expression that has been commonly used since the beginning of the Fifth Republic to characterize an area of action of the President of the Republic that could not be shared with the other components of the Executive Branch, i.e., the Prime Minister. In the author's view, the latter had its own "reserved domain," of which telephone tapping was a part.
8. The source text in French is as follows: « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ».
9. In France, since the French Revolution there have been two kinds of jurisdiction: "judicial jurisdictions" (i.e., the courts) and "administrative jurisdictions" called "autorités administratives indépendantes" (AAI), whose number amounts to 17 and whose aim, broadly speaking, is to judge the Administration. Unlike the courts, which are composed solely of Judges, the AAIs are composed of both Judges and people who are not Judges, mainly Parliamentarians and high-ranking civil servants. The CNCIS was an AAI. Some European jurisdictions deny that some AAIs are actual jurisdictions.
10. A qualified person ("personnalité qualifiée") is a term used in the French Administration to appoint an individual in a body because of his or her skills and background as opposed to his or her position or professional status (e.g., judge, parliamentarian, police officer, military officer, etc.). In this instance, the qualified person must be a civil servant who is a high-level engineer specialized in telecommunications and IT.
11. Since the enactment of the Act, the expression commonly used was "boîte noire" (blackbox). It refers to algorithms built with selectors to detect suspicious regex and keywords within the flows of communication. The suspicious regex and keywords are established in relation with the purposes defined in the 2015 Act (*see* Section III, *infra*).
12. Vincent Lamigeon, *Gina Haspel, ex-directrice de la CIA* : "*La DGSE est dans le top-3 mondial*" [Gina Haspel, former director of the CIA : "The DGSE is in the top-3 in the world"], Challenges (June 24, 2022), https://urlz.fr/iHFD.
13. Dépêche AISG n° 4926, 13 December 2011.
14. *Décision n° 2015-713 DC*, 23 July 2015, accessed at https://www.conseil-constitutionnel.fr/decision/2015/2015713DC.htm
15. *Id.*
16. Avis Consultatif, *Avis sur la mise en place d'un dispositif visant à vérifier l'existence de menaces pour les intérêts fondamentaux de la Nation...* [Opinion on the establishment of a mechanism to verify the existence of threats to the fundamental interests of the Nation...], Conseil d'État (24 May 2018), https://www.conseil-etat.fr/avis-consultatifs/derniers-avis-rendus/au-gouvernement/avis-sur-la-mise-en-place-d-un-dispositif-visant-a-verifier-l-existence-de-menaces-pour-les-interets-fondamentaux-de-la-nation#anchor1.
17. Décision de Justice, *Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité* [Connection data : the Council of State reconciles compliance with European Union law and the effectiveness of the fight against terrorism and crime], Conseil d'État (21 April 2021), https://urlz.fr/i7ls.
18. CNCIS, *1er rapport d'activité 1991-1992*, Paris, La documentation française, 1993, p. 237.
19. Out of a total of 66.72 million inhabitants.
20. Out of a total of 67.39 million inhabitants.