COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

9th Activity Report
2024

In memory of Serge Lasvignes (1954-2025)

Chairman of the CNCTR from October 2021 to January 2025

Foreword

The National Oversight Commission for Intelligence-Gathering Techniques (CNCTR) is required by law to produce an activity report. It is made public and is intended for a general audience. Since its inception, it has reported on the commission's activities without breaching national defence secrecy. More importantly, it seeks to ensure that intelligence-gathering techniques are used in a manner that strikes the balance required by law between respect for privacy on the one hand and the defence and promotion of the fundamental interests of the nation on the other.

As Chairman of the CNCTR from October 2021 to 31 January 2025, Serge Lasvignes paid particular attention to this balance and to how it should be reported. He highlighted the key factors that attest to this balance, as well as the risks that could undermine it and the legal and technical uncertainties that weaken it. He supplemented each year's report with thematic studies, providing insight and perspective.

Serge Lasvignes remained in office until illness forced him to step down. He passed away on 15 February 2025. The members of the CNCTR and its staff pay tribute to his memory with affection and respect and dedicate this activity report to him.

2024: Controlled activity in a exceptional year

The most striking observation about 2024 is that it did not see an explosion in the use of intelligence-gathering techniques, despite the exceptional nature of the events, both planned and unplanned, that marked it: European and then legislative elections, the Olympic torch relay and the 2024 Olympic and Paralympic Games in Paris, the reopening of Notre-Dame Cathedral in Paris, riots and a state of emergency in New Caledonia, and violent unrest in Martinique and Guadeloupe.

The CNCTR has adapted its activities to this extraordinary year. While the number of inspections carried out within the services

decreased only slightly, from 136 in 2023 to 123 in 2024, the period of the Games was avoided as much as possible and more controls were conducted remotely. Nevertheless, the number and quality of thematic discussions with the intelligence services, either on their own initiative or at the Committee's request, have not declined. The commission considers this to be an essential part of its relationship with these services. At times, they help to gain a deeper understanding of a threat or phenomenon that guides the action of the services; at other times, they help the commission to develop a broader perspective, beyond the necessarily one-off nature of controls, often with the aim of identifying possible technical improvements or desirable adjustments to operational doctrine.

In this context, the number of requests for the use of intelligence-gathering techniques examined by the commission rose only slightly, from just under 95,000 in 2023 to just under 99,000 in 2024, and the number of persons under surveillance remained constant: 24,209 in 2023 and 24,308 in 2024, according to the commission's estimates. The proportion of negative opinions issued by the commission was almost identical: 1.2% in 2023 and 1.3% in 2024. Although the number of "telephone tapping" operations was temporarily increased, this was within the limits recommended by the CNCTR.

These findings show that the intelligence services, under the authority of the public authorities, the aegis of the National Coordination of Intelligence and the Fight against Terrorism and the control of the CNCTR, have kept the situation under control and maintained a measured and selective approach.

However, the particular events of 2024 have left their mark on the objectives of the intelligence services. Prevention of terrorism once again became the primary reason for surveillance in terms of the number of people involved in 2024, after organised crime had been the primary reason for the first time in 2023.

Persistent anomalies ten years after the Intelligence Act

The relationship of trust that the CNCTR enjoys with the intelligence services does not exempt it from once again pointing out the persistence of anomalies. The most serious of these concern the use of data collected in "intelligence reports". These bulletins are essential for assessing the usefulness and legal justification of surveillance measures after they have been authorised. They also make it possible to verify that the information retained after the raw data has been deleted at the end of the legal retention period is indeed relevant to the purpose for which it was collected. However, this information is not always found where and when it should be. Similarly, the imperfect retention of accurate records of operations carried out or, more rarely, the expiry of the period of validity of an authorisation to use an intelligence-gathering technique or ignorance of the limits set by the commission in its opinion on a request from a service are still among the anomalies noted by the commission.

The CNCTR reiterates its confidence in the intelligence services and their compliance with the law. It is also aware of the difficulties they face, the operational priorities they have to meet and the efforts required to ensure consistent compliance with the legal framework across the board. It therefore invites them to implement specific, shared and monitored action plans to ensure, effectively and sustainably, that the law is properly applied by all and that the commission, through its controls, dialogue with them and the development of its doctrine, is able to fully monitor this.

Expected developments

For the same purpose, the CNCTR has high expectations for the implementation of the decision taken by the President of the Republic at the end of 2023 to centralise all data resulting from computer data collection (RDI) within the Inter-Ministerial Control

Group (GIC). This technique, which takes various forms, is particularly intrusive. However, it is both increasingly used and difficult to control when its traces are scattered across different services.

The commission emphasises that centralisation must, in equal measure, enable it to effectively control the RDI and provide intelligence service agents with a unified and more accessible working tool, while strengthening the role of the GIC.

As agreed, technical studies began in autumn 2024, under the leadership of the National Coordination of Intelligence and the Fight against Terrorism, once the Paris Olympic Games were over. Significant resources and sustained efforts are essential to ensure that the system is in place by mid-2027, as decided. The commission is paying very close attention to this; 2025 and 2026 will be decisive years.

A year of parliamentary initiative

In terms of legislation and parliamentary activity, 2024 was marked first and foremost by the law of 25 July 2024 aimed at preventing foreign interference in France[1]. Secondly, it saw the publication of a report by a Senate commission of inquiry on the impact of drug trafficking in France[2] and the tabling of a bill on the same subject[3].

A common feature of these two texts is that they provide for the extension of the intelligence-gathering technique known as the algorithm, introduced into the French Internal Security Code by the 2015 law for the purpose of combating terrorism, to the detection respectively of foreign interference and drug trafficking.

1. See law no. 2024-850 of 25 July 2025 on preventing foreign interference in France.
2. Senate, 7 May 2024, report no. 588 on behalf of the commission of enquiry into the impact of drug trafficking in France and the measures to be taken to remedy it; Chairman: Mr Jérôme Durain, rapporteur: Mr Étienne Blanc.
3. Senate, 12 July 2024, bill no. 735 rect. aimed at freeing France from the trap of drug trafficking, presented by Mr Étienne Blanc and Mr Jérôme Durain, senators.

In both cases, Parliament found the increase in threats to be a legitimate justification for the use of this particular technique.

This report takes this opportunity to set out the legal framework for algorithms in a dedicated study. It is important to dispel the fears raised by the very term "algorithm". What the French Internal Security Code allows is neither mass surveillance nor automation. The CNCTR's control at each stage, in particular to authorise an algorithm project, then to issue opinions on each lifting of anonymity after possible detections resulting from algorithmic processing and, finally, on the request to implement intelligence-gathering techniques against the people involved, protects against the risk of mass surveillance. The examination by the service and then by the commission of the merits of each detection and the consequences to be drawn preserves the principle of human primacy[4] and protects against the risk of outright automation.

An important decision by the ECHR and questions still pending

In terms of case law, 2024 saw the European Court of Human Rights deliberate on a long-awaited decision, as it ruled on applications lodged in 2015 and 2017[5].

After a very detailed examination, the ECHR's decision recognised that the French legal framework guarantees everyone the right to an effective remedy against the use of intelligence-gathering techniques against them. The Court ruled, in particular, on the independence of the CNCTR and the effectiveness of its oversight, as well as on the proper coordination between the prior complaint procedure before the CNCTR and the subsequent appeal before a specialised panel of the Council of State.

4. See in particular: Council of State, study at the request of the government, "Artificial intelligence and public action: building trust, serving performance", 31 August 2022.

5. See section 3.1 of the activity report.

This decision can be seen as confirmation that French law and practice provide a balanced framework for public intelligence policy, respecting both freedoms and the defence and promotion of the fundamental interests of the Nation. This was also the conclusion reached in 2024 by two useful symposiums co-organised by the CNCTR[6].

However, the legal and operational landscape of intelligence is not without its shortcomings and weaknesses. For example, it should be emphasised once again that France has no legal framework for the exchange of information between national and foreign services. This is clearly contrary to international case law[7]. In a world of global threats, such exchanges are legitimate and indispensable. Giving them legal status is no less so; rights and freedoms cannot be guaranteed on one side alone.

Ten-year anniversary and future outlook

The year 2025 marks the tenth anniversary of the Intelligence Act of 24 July 2015, which introduced Book VIII of the French Internal Security Code and established the National Oversight Commission for Intelligence-Gathering Techniques. It is therefore also the anniversary of the establishment of the commission, following on from the National Commission for the Control of Security Interceptions.

These ten years have both put our country to the test with serious attacks and risks and confirmed the effectiveness of a legal framework that has only needed to be modified marginally.

For the commission, which also believes it has fulfilled its mission, this is less an opportunity for self-congratulation than for reflection,

6. International conference co-organised by the CNCTR and the journal Etudes françaises de renseignement et de cyber: "The challenges of intelligence oversight: a dialogue between oversight bodies?", Paris, 15 October 2024 – National Commission for Information Technology and Civil Liberties, "Futures, innovations, revolutions 2024": "Surveillance in all its forms: what ethics for (protecting) our freedoms", Paris, 19 November 2024.

7. see in particular: ECHR 25 May 2021, Big Brother Watch and others v. United Kingdom, application nos. 58170/13, 62322/14 and 24960/15.

in conjunction with the French intelligence community, parliamentary representatives and all those who have shown an interest in the debate.

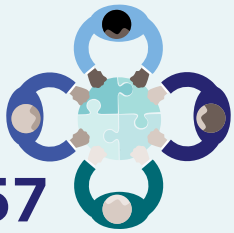
At least two areas deserve consideration. The first is the legal principle of proportionality. This principle is put to the test by technology, as the use of the most intrusive intelligence-gathering techniques occurs earlier and generally increases. The principle also applies to the duration of surveillance, which can be questioned when it is renewed only while awaiting decisive evidence. The very nature of administrative policing in the field of intelligence is to investigate in order to prevent. Public action is therefore carried out amid hypothetical scenarios and exposed to the risk of uncertainty. However, whether from a technical or a time-related perspective, one must neither endure the situation nor become accustomed to it.

The second area concerns cooperation between the commission and the intelligence services from both circles. It is a solid achievement built over ten years; it must be maintained. The commission invites the intelligence services to participate at all stages: justification of requests for intelligence-gathering techniques, to ensure that they are properly assessed; availability during ex post controls, to ensure their usefulness and enable effective follow-up; thematic exchanges, to overcome the asymmetry of technical knowledge, understand the risks that the services are responsible for preventing and identify points of doctrine that require clarification or development. As the guarantor of intangible rights and of the legal action of the intelligence services, which are responsible for protecting against changing and often growing threats, the CNCTR hereby renews its commitment.

Vincent Mazauric
State Councillor,
Chairman of the CNCTR

2024 Key figures

98,883
requests for intelligence-gathering techniques
(individual domestic techniques)*



157
collegial meetings

24,308
people under surveillance

123
controls
in the divisions

€3.4 million
in budget

* This data does not include non-individualised requests and/or requests relating to international electronic communications surveillance measures which covers requests relating to the technique known as the algorithm provided for in Article L. 851-3 of the French Internal Security Code, requests for the transmission of intelligence subject to prior notification to the commission referred to in II of Article L. 822-3 of the same code or the authorisations for use referred to in its Article L. 854-2 (see respectively p. 42 and p. 49 below).

10 travels
within the territories,
including **one overseas department**

9 members
(4 women, 5 men)
4 of which are full-time members

22 agents
(on 31/12/2024)

- 11 men / 11 women,
- 13 public agents / 9 contract agents,
- average age of 39 years.

2024 Activity Report

Part 1. The state of surveillance in 2024: a stabilisation in the number of persons under surveillance combined with a moderate increase in surveillance despite exceptional security challenges

As provided for in Article L. 833-9 of the French Internal Security Code, the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR) reports annually on the fulfilment of its mission to ensure that intelligence-gathering techniques are implemented in accordance with the legal framework governing them. To this end, it provides information on its control activities, in as much detail as national defence secrecy allows, and informs the public of its findings on the use of intelligence-gathering techniques by the services in relation to persons present on the national territory.

Put into perspective over a five-year period, these figures relate to the number of persons under surveillance, the purposes[1] invoked in support of requests for intelligence-gathering techniques submitted to the commission and the number of opinions issued on these requests for authorisation.

1. The provisions of Article L. 811-3 of the French Internal Security Code list seven purposes: para. 1) of this article, "National independence, territorial integrity and national defence" (purpose 1); 2) "the major interests of foreign policy, the execution of France's European and international commitments and the prevention of any form of foreign interference" (purpose 2); 3) "the major economic, industrial and scientific interests of France" (purpose 3); 4) "the prevention of terrorism" (purpose 4); 5) "the prevention of: a) Damage to the republican form of the institutions; b) Actions aimed at maintaining or rebuilding dissolved groups pursuant to Article L. 212-1; c) Collective violence likely to seriously harm public peace" (purpose 5a/5b/5c); 6, "prevention of organised crime and delinquency; and 7) "prevention of the proliferation of weapons of mass destruction".

The commission also reports on the number of preliminary opinions it issued in 2024 on requests relating to the surveillance of international electronic communications.

The statistical data presented in this report is the result of data extraction and aggregation carried out by the CNCTR in conjunction with the Inter-Ministerial Control Group (GIC), followed by data validation.

As in 2023, 2024 was marked by a very high level of threats to France against a backdrop of intense geopolitical tensions (war on European soil in Ukraine since February 2022, conflict in the Middle East since October 2023, etc.). Added to this context was **an exceptional domestic situation raising significant security issues, in particular the organisation of the 2024 Olympic and Paralympic Games in Paris, preceded by the Olympic torch relay in May 2024.** However, in addition to this extraordinary event, it is also worth noting **unprecedented levels of collective violence in New Caledonia, then in the French West Indies and finally, in December 2024, the reopening of Notre-Dame Cathedral in Paris**, which led to the presence in the capital of several dozen heads of state and government.

The practices of intelligence services in terms of technical surveillance change in response to threats and instability, but also in line with technological developments, which sometimes call into question the usefulness of certain techniques due to their unsatisfactory effectiveness.

In this context, the shift towards more intrusive techniques already observed in previous years continued in 2024, with, in particular, **increasing use of the quota-free technique of collection and recording computer data (RDI)**, provided for in Article L. 853-2 of the French Internal Security Code. However, this increasing use of the most intrusive techniques has not been **accompanied by a significant decrease in the use of "traditional" techniques** such as

security interceptions, provided for in Article L. 852-1 of the French Internal Security Code.

Overall, despite a truly exceptional year in terms of security challenges and a significant increase in the activity of certain services in the context of the organisation of the 2024 Olympic and Paralympic Games in Paris, the CNCTR notes **an overall stabilisation in the number of persons under surveillance**, with divergent trends depending on the purpose for which the surveillance is carried out (1.1). **This stabilisation is also reflected in the number of intelligence-gathering techniques requested**, although this should not mask a **significant increase in requests for the most intrusive techniques**, reinforcing a trend already observed in recent years (1.2). The purposes cited in support of these requests remain similar to those of previous years (1.3)

1.1. A stabilisation in the number of persons under surveillance should not mask divergent trends depending on the purpose for which the surveillance is carried out

As it has done since its first activity report, the commission has estimated the number of persons who were subject to at least one intelligence-gathering technique in 2024, among those provided for in Chapters I to III of Title V of Book VIII of the French Internal Security Code.

This does not include authorisations to access connection data in real time, which are limited to identifying subscribers and recording subscription numbers[2].

After increasing by nearly 15% in 2023, **the number of persons under surveillance stands at 24,308** this year, representing an increase of only 0.4% compared to 2023 and 10.7% compared to the period prior to the health crisis linked to the COVID-19 pandemic.

	2020	2021	2022	2023	2024	2023/2024 change	2020/2024 change
Number of persons under surveillance	**21,952**	**22,958**	**20,958**	**24,209**	**24,308**	**+0,4%**	**+10,7%**
For terrorism prevention purposes	**8,786** (40% of the total)	**7,826** (34.1% of the total)	**6,478** (30.9% of the total)	**6,962** (28.8% of the total)	**7,264** (29.9% of the total)	**+4,3%**	**-17,3%**
For purposes linked to the prevention of organised crime and delinquency	**5,021** (22.9% of the total)	**5,932** (25.8% of the total)	**5,471** (26.1% of the total)	**7,058** (29.2% of the total)	**6,761** (27.8% of the total)	**-4,2%**	**+34,7%**
For the purpose provided for in Article L. 811-3 (5) of the French Internal Security Code	**3,238** (14.8% of the total)	**3,466** (15.1% of the total)	**2,692** (12.8% of the total)	**2,551** (10.5% of the total)	**2,528** (10.4% of the total)	**- 0,9%**	**- 21,9%**

As highlighted in previous reports, the results of this calculation have a margin of uncertainty of around 10% (see the 8th activity report of the commission, p. 30[3] on this point).

The stabilisation in the number of persons under surveillance is mainly due to the refocusing of part of the services' activities on the objective of preventing terrorism in the context of the organisation

2. The CNCTR considers that the identification of subscribers and the listing of subscription numbers, provided for in the second paragraph of Article L. 851-1 of the French Internal Security Code, are not so much a surveillance measure per se as a prerequisite for surveillance measures. Such measures begin, in the commission's view, as soon as "phone records" are obtained from the person concerned pursuant to the first paragraph of the same article L. 851-1 of the same code.

3. The processing of requests for intelligence-gathering techniques uses different applications, which leads to the aggregation of data that is still not completely harmonised. Furthermore, service requests are presented based on the intelligence-gathering technique, as defined by the French Internal Security Code, and not on the individual concerned. Furthermore, the persons concerned are not always named or precisely identified.

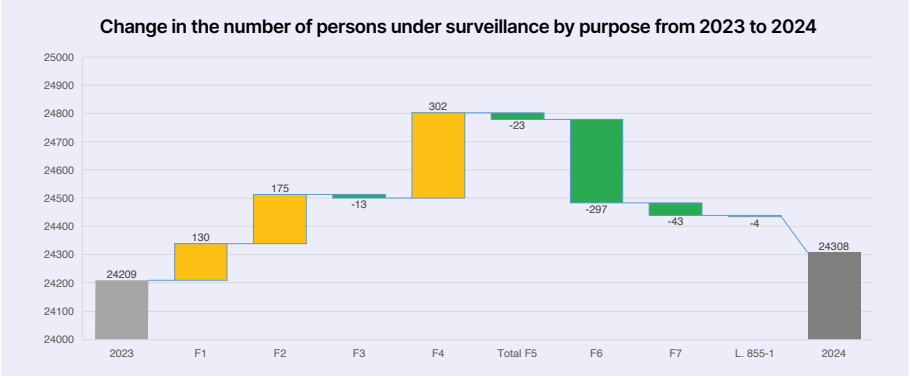
of the 2024 Olympic and Paralympic Games in Paris (see figures in section 1.1.1).

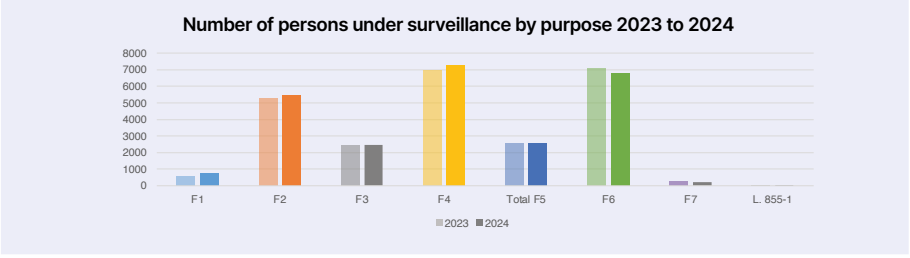
Thus, **the year 2024 was marked by increased investment by the intelligence services in the prevention of terrorism, the prevention of interference, and the protection of national independence, territorial integrity and national defence**. The increase in the number of persons under surveillance for these purposes was accompanied by a decrease in the number of persons under surveillance for the prevention of organised crime and delinquency, although in both cases the variations were modest (1.1.1).

Furthermore, **the prevention of various forms of violent activism** (purposes mentioned in paragraph 5 of Article L. 811-3 of the French Internal Security Code), an area where the issue of protecting privacy is compounded by the issue of protecting freedom of expression, opinion, association and demonstration, **has seen a slight decrease for the third consecutive year** (1.1.2).

1.1.1. In 2024, terrorism prevention once again becomes the primary reason for surveillance in terms of the number of people involved

The graphs below show both the distribution of the variation in the number of persons under surveillance according to the different purposes and the change in this number for each of these purposes between 2023 and 2024.





(P1): national independence, territorial integrity and national defence;

(P2): the major interests of foreign policy, the execution of France's European and international commitments and the prevention of any form of foreign interference;

(P3): the major economic, industrial and scientific interests of France; (P4): the prevention of terrorism;

(P5): the prevention of: a) Damage to the republican form of the institutions; b) Actions aimed at maintaining or rebuilding dissolved groups; c) Collective violence likely to seriously harm public peace;

(P6): the prevention of organised crime and delinquency;

(P7): the prevention of the proliferation of weapons of mass destruction;

L. 855-1: purpose specific to prison intelligence-gathering services, provided for in Article L. 855-1 of the French Internal Security Code, pertaining to the prevention of prison breaks and security inside prisons or health facilities meant to receive prisoners.

The year 2023 saw a significant increase in the number of persons under surveillance for the prevention of organised crime and delinquency (+29% compared to 2022), making this the main reason for surveillance in terms of the number of people involved. Over the same period, the number of persons under surveillance for the prevention of terrorism increased by a more modest 7.5%.

In 2024, in the **context of an increase in both exogenous and endogenous threats, in the** context of the staging of the Olympic and Paralympic Games, the **purpose mentioned in Article L. 811-3(4) of the French Internal Security Code once again becomes the primary reason for surveillance both in terms of the number of people involved and the techniques implemented** (see point 1.3 below). At the same time, the number of persons under surveillance for the purposes mentioned in paragraph 6 of the same article fell, albeit only slightly (-4.2%).

Furthermore, the prevention of organised crime and delinquency is the reason for surveillance that has seen the greatest increase in the number of people involved over the last five years (+18.8%, corresponding to 6,761 people kept under surveillance for this reason in 2024 compared with 5,693 in 2019).

A very unstable international geopolitical situation also explains the **continued increase in the number of persons under surveillance for the purpose of defending and promoting major foreign policy interests**, fulfilling France's European and international commitments and **preventing any form of foreign interference** (+ 3.3% between 2023 and 2024).

1.1.2. The number of persons under surveillance for the prevention of various forms of violent activism continues to fall

Continuing the trend observed since 2021, the decline in the number of persons under surveillance for the purposes mentioned in Article L. 811-3(5) of the French Internal Security Code is confirmed in 2024 with a decrease of 0.9% compared to 2023 (compared to the decrease of 5.2% between 2022 and 2023). The **number of persons under surveillance for this purpose has reached its lowest level since 2018**[4].

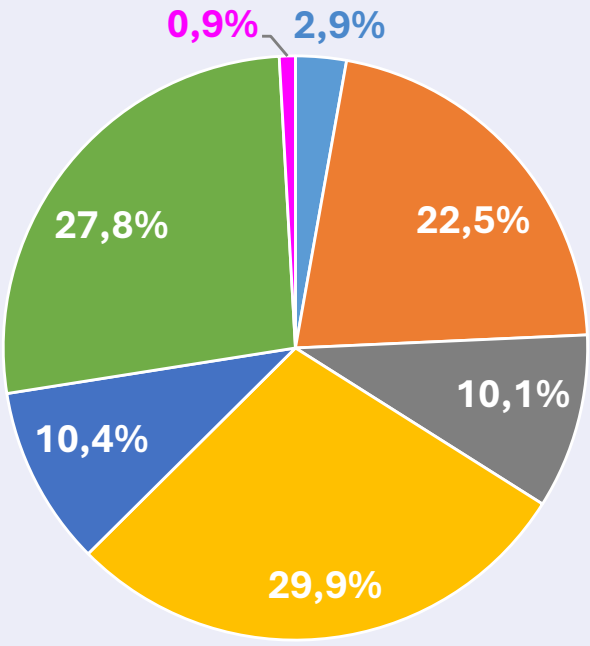
As in 2023, this change is linked to the continuing significant increase in the number of requests for additional information made by the commission (see point 1.2.4 below), which have contributed to continuing the dialogue established since 2022 with the intelligence services on the scope of this purpose[5]. These exchanges have made it possible to better identify the people who warrant surveillance, leading to a corresponding stabilisation in the rate of negative opinions issued in this area.

In addition, the number of persons under surveillance for the defence and promotion of France's major economic and industrial interests has stabilised at around the level seen before the health crisis linked to the COVID-19 pandemic.

4. 2,116 persons were under surveillance under this heading in 2021 (6th CNCTR activity report 2021, p. 73).

5. On this point, see the study on the surveillance of violent extremism in the 7th activity report 2022 of the CNCTR, p. 75 et seq.

Breakdown of persons under surveillance by reason for surveillance



- National independence, territorial integrity and national defence
- The major interests of foreign policy, the execution of France's European and international commitments and the prevention of any form of foreign interference
- The major economic, industrial and scientific interests of the France
- The prevention of terrorism
- The prevention of: a) Damage to the republican form of the institutions; b) Actions aimed at maintaining or rebuilding dissolved groups; c) Collective violence likely to seriously harm public peace
- The prevention of organised crime and delinquency
- The prevention of the proliferation of weapons of mass destruction

Note: As the same person may be under surveillance for several purposes, the aggregate of the various percentages presented exceeds 100%.

1.2. A moderate increase in the number of requests for intelligence-gathering techniques, with, however, greater use of the most intrusive techniques

Despite a high level of threats and the organisation of the Olympic and Paralympic Games, **the number of requests for the use of intelligence-gathering techniques on national territory rose by a moderate 3% on the previous year to 98,883 requests**[6]. While the number of persons under surveillance has stabilised, this increase reflects a slight rise in the average number of techniques requested for each person under surveillance.

The observation of this relative stability in the number of techniques requested can be explained by the fact that while the activity of certain services increased in the run-up to and during the period of the Olympic and Paralympic Games, this increase was initially based on a temporary reallocation of some of their human and technical resources for the purpose of anticipating threats likely to target this event.

The CNCTR issues an opinion on each request to implement an intelligence-gathering technique on national territory before the Prime Minister takes a decision authorising or refusing its implementation[7]. It must give its opinion within twenty-four hours when a request comes under the competence of a member with the status of magistrate[8] and ruling alone. This time limit is extended to seventy-two hours when the request requires

6. This figure covers so-called "individualised' techniques and therefore does not include requests based on Article L. 851-3 of the French Internal Security Code (the so-called algorithm technique), nor transmissions between services covered by an authorisation from the commission.

7. See the CNCTR's 7th 2022 activity report, p. 132.

8. Members referred to in Article L. 831-1 (2) and (3) of the French Internal Security Code.

examination by a collegial, plenary or restricted committee[9]. The commission endeavours to comply with these time limits. A "priority" procedure has also been introduced to meet operational needs requiring very urgent processing of requests[10].

The opinions issued break down as shown in the table below. These figures include all the requests submitted by the intelligence services during the years 2020 to 2024[11]. They show the changes in the way the services use each category of technique over five years and from one year to the next.

	2020	2021	2022	2023	2024	2023 / 2024 change	2020 / 2024 change
Access to recorded internet connection data (identification of subscribers and the index of subscription numbers) (Article L. 851-1 of the French Internal Security Code)	30,758	32,254	31,427	33,657	34,612	+2,8%	+12,5%
Access to recorded internet connection data (other requests, including linked to "phone records") (Article L. 851-1 of the French Internal Security Code)	18,006	19,974	19,263	21,430	22,493	+5%	+24,9%
Real-time access to internet connection data (Article L. 851-2 of the French Internal Security Code)	1,644	1,534	1,175	763	731	-4,2%	-55,5%
Real-time geolocation (Article L. 851-4 of the French Internal Security Code)	8,394	9,920	10,901	10,982	9,909	-9,8%	+18%

9. In accordance of the provisions of Article L. 832-3 of the French Internal Security Code, the collegial committees of the commission shall in particular deal with any new or serious question. The board meets in plenary session at least once a month and is particularly competent to hear requests relating to protected professions within the meaning of Article L. 821-7 of the French Internal Security Code.

10. This procedure enables the commission to issue opinions within less than an hour.

11. The data shown in the table does not include non-individualised requests and/or requests relating to international electronic communications surveillance measures which covers requests relating to the technique known as the algorithm provided for in Article L. 851-3 of the French Internal Security Code, requests for the transmission of intelligence subject to prior notification to the commission referred to in II of Article L. 822-3 of the same code or the authorisations for use referred to in its Article L. 854-2 (see respectively p. 42 and p. 49 below).

	2020	2021	2022	2023	2024	2023 / 2024 change	2020 / 2024 change
Security interceptions through the Inter-Ministerial Control Group (Article L. 852-1 of the French Internal Security Code)	12,891	12,736	12,798	13,021	14,316	+9,9%	+11,1%
Tapped communications using IMSI catcher (II of Article L. 852-1 of the French Internal Security Code)	0	0	0	0	0	-	-
Security interceptions on exclusively wireless networks (Article L. 852-2 of the French Internal Security Code)	0	3	5	10	5	-50%	-
Collecting of correspondence sent or received through satellite (Article L. 852-3 of the French Internal Security Code)	0	0	0	0	1	-	-
Location of people or objects ("geolocation devices") (Article L. 851-5 of the French Internal Security Code)	1,598	2,006	1,951	2,084	2,065	-0,9%	+29,2%
Collecting of internet connection data using IMSI catcher (Article L. 851-6 of the French Internal Security Code)	311	583	641	607	616	+1,5%	+98,1%
Recording of words spoken in a private capacity and recording of images in a private setting (Article L. 853-1 of the French Internal Security Code)	1,564	2,138	3,314	3,802	3,912	+2,9%	+150,1%
Collection and recording of computer data (Article L. 853-2 of the French Internal Security Code)	2,418	3,758	4,260	4,493	5,715	+27,2%	+136,4%
Entering of private places (Article L. 853-3 of the French Internal Security Code)	2,021	2,682	3,767	4,053	4,508	+11,2%	+123,1%
All requests for intelligence-gathering techniques	79,605	87,588	89,502	94,902	98,883	+4,2%	+24,3%

1.2.1. The trend for intelligence services to use more intrusive intelligence-gathering techniques is confirmed and strengthened in 2024

The moderate increase in the number of requests for the implementation of techniques noted in 2024 does not call into question the dynamic observed for several years of increasingly frequent use of the most intrusive techniques.

Indeed, **the most notable increase in 2024 concerns the technique of collection and recording of computer data (RDI)[12] for which the number of requests increased by more than 27% in 2024 compared to the previous year**, following an increase of 5.5% in 2023 and 13.4% in 2022.

This increase cannot be explained solely by the exceptional context of the organisation of the Olympic and Paralympic Games. The CNCTR sees it as a well-established trend of increasing use of this technique, in particular to compensate for the limitations of security interceptions. The use of RDI can help overcome the difficulties associated with the ever-increasing use of encrypted channels for communication. The number of RDI requests has jumped by more than 136% during the five-year period from 2020 to 2024.

For the other most intrusive techniques, the increase in requests is less marked but follows a growth dynamic that has not abated since 2020.

For example, **recording of words spoken in a private capacity or recording of images in a private setting** techniques rose by 2.9% in 2024, bringing the increase to more than 150% over the last five years.

12. See the provisions of article L. 853-2 of the French Internal Security Code.

Consistent with the increase in the use of techniques for collecting computer data or recording words or images, requests for **entering private places**, which is not a surveillance technique as such, but a "support" technique necessary for the implementation of intelligence-gathering techniques proper, increased significantly, by more than 11% in 2024.

In addition, after a moderate fall in 2023, requests for **connection data collection by *IMSI catcher*** increased very slightly by 1.5% in 2024, highlighting a stabilisation in the use of this technique by services over the last four years. This stability is undoubtedly linked to the fact that, as with security interception, this technique is subject to a quota system by virtue of the provisions of article L. 851-6 of the French Internal Security Code.

Finally, a new authorisation for the implementation of automated processing to detect connections likely to reveal a terrorist threat (the so-called **algorithm** technique, provided for in article L. 851-3 of the French Internal Security Code[13]) was issued in 2024, bringing to six the number of algorithms authorised since this technique was opened up to intelligence services in 2015. One of them was abandoned in 2024. However, the option opened up by law no. 2021-998 of 30 July 2021 on the prevention of terrorist acts and intelligence, which allows the extension of algorithm-based techniques to complete internet resource addresses (Uniform Resource Locators, URLs)[14], as well as the option to use this technique for purposes other than the prevention of terrorism, introduced by law no. 2024-850 of 25 July 2024 aimed at preventing foreign interference in France[15], have, however, not yet been implemented.

13. See the study devoted to this technique on p. 98 - Study - The algorithm: from fantasy to legal reality.

14. See article 15 of the law amending Article L. 851-3 of the French Internal Security Code.

15. See Article 6 of the law which temporarily modifies, until 1 July 2028, the provisions of Article L. 851-3 of the French Internal Security Code in order to open up the technique to the purposes mentioned in Article L. 811-3(1) and (2) of the same code in order to prevent foreign interference and threats to national defence.

1.2.2. The use of less intrusive "traditional" techniques has not diminished

Despite the use of more intrusive techniques, particularly RDI, so-called traditional intelligence-gathering techniques are not being abandoned by the intelligence services. On the contrary, their status as first-line techniques is being reinforced, insofar as they help justify the relevance of placing a person under surveillance or provide a better understanding of their environment.

Further increase in requests for access to internet connection data

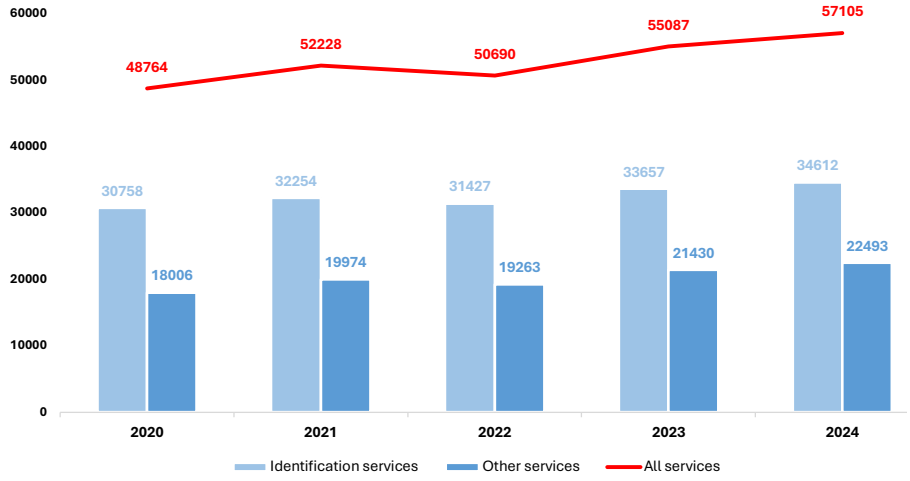
After a dip in 2022, the number of requests for access to recorded internet connection data continued to rise in 2024 (up 3.7% on 2023). Requests for this type of access, which is less intrusive than the other techniques provided for in the French Internal Security Code, will account for more than half of all requests for intelligence-gathering techniques made by the intelligence services in 2024.

On this point, the past year does not represent a break with previous years. In fact, as noted in the commission's activity report for 2023, access to internet connection data is a first-line surveillance technique enabling the services to gain a better understanding of the target individual's environment.

This high proportion of requests for access to internet connection data in the total number of requests for intelligence-gathering techniques made by the intelligence services is an important indicator to monitor. Its stability shows that the intelligence services have integrated and continue to apply a principle of subsidiarity in the use of intelligence-gathering techniques, consisting in particular of progressing by stages in the surveillance of a person. However,

the first stage of surveillance still mainly involves obtaining internet connection data, which is very useful for starting an investigation and assessing the need to continue it, but less revealing of the private lives of the persons under surveillance.

Change in the breakdown of requests for access to internet connection data between 2020 and 2024



On the other hand, requests for **access to real-time internet connection data** continue to fall: - 4.2% in 2024, after falling by 35% in 2023 and 23% in 2022, seeming to support the analysis that limiting this technique to the purpose relating to the prevention of terrorism is leading services to favour other, sometimes more intrusive, techniques for the other purposes set out in the French Internal Security Code.

An increase in the use of security interceptions

Even if their contribution is less than in the past in terms of intelligence in the strict sense, one of the notable facts of 2024 resides in **the significant increase in requests for security interceptions** ("*telephone tapping*"), implemented *via* the Inter-Ministerial Control Group (GIC) on behalf of the intelligence services, **by almost 10% in 2024** compared with the previous year, following a more moderate increase of 1.7% in 2023.

This trend highlights that the technique remains of interest to the services in order to improve their knowledge of a person under surveillance and to prepare for the use of other, more intrusive techniques if the interest it presents is verified. In this respect, it should be noted that for the first time since 2019, the Prime Minister has temporarily increased the number of interceptions that may be carried out simultaneously in 2024 and then permanently at the beginning of 2025[16].

A CHANGE IN THE SECURITY INTERCEPTIONS QUOTA FOR THE FIRST TIME SINCE 2019

Security interceptions, provided for under Article L. 852-1 of the French Internal Security Code, are one of the four so-called "*domestic*"[17] techniques subject to a quota system, under which the number of authorisations simultaneously in effect cannot exceed a maximum set by decision of the Prime Minister, following an opinion from the CNCTR.

This quota system is intended to ensure that the services use these techniques only ***"in cases of public interest necesity as provided for by law"***[18].

16. See box below.

17. The other domestic techniques subject to a quota system are access to internet connection data in real time (Article L. 851-2 of the French Internal Security Code), the collection of internet connection data by IMSI catcher (Article L. 851-6 of the French Internal Security Code) and the interception of correspondence through satellite (Article L. 852-3 of the French Internal Security Code).

18. See article L. 801-1 of the French Internal Security Code.

Already provided for by law no. 91-946 of 10 July 1991 on the secrecy of correspondence sent by electronic communications, the quota of security interceptions that may be granted simultaneously had not been modified on the date of entry into force of law no. 2015-912 of 24 July 2015 on intelligence and remained fixed at 2,700. It was subsequently increased three times in 2017, 2018 and 2019, to finally reach 3,800.

In 2024, for the first time since 2019, the commission received two proposals from the Prime Minister to increase the quota for security interceptions:

at the beginning of the year, it was presented with a proposal for a temporary increase in this quota in the context of the organisation of the 2024 Olympic and Paralympic Games,

At the end of the year, it was presented with a proposal for a permanent increase based on the high level of the threat to which France is exposed.

In two classified deliberations, the CNCTR deemed it necessary to temporarily increase the quota set for 2019 in the exceptional context of the Olympic and Paralympic Games, which could exacerbate an already very high level of threat. On the other hand, it accepted that, beyond the impact of this particular event, the level of both exogenous and endogenous threat to the country justified a permanent increase in this quota, albeit to a lesser extent.

Changes in the security interceptions quota since 2015

Ministry responsible:	2015	2017	2018	2019	2024 (temporary quota)	From 1 October 2024	2025
Ministry of the Interior	2,235	2,545	3,000	3,050	3,750	3,100	3,350
Ministry of Defence	320	320	400	550	600	550	600
Ministry of the Economy and Budget (customs, Tracfin)	145	145	150	150	130	130	130
Ministry of Justice	-	30	50	50	20	20	20
Total	2,700	3,040	3,600	3,800	4,500	3,800	4,100

As in 2023, the **use of techniques for locating people or objects** ("tracking devices") remains stable over the last five years with a volume of around 2,000 requests per year.

Furthermore, while requests for **real-time geolocation** appear to have fallen significantly, by almost 10% in 2024, this development needs to be put into perspective. At the end of 2023, a software change was made for submitting these requests, allowing the services to file a single geolocation request for the various technical identifiers belonging to the same person, instead of submitting one request per identifier. The drop in the number of requests observed in 2024 does not therefore reflect less use of the technique.

Generally speaking, these developments show that the intelligence services are adapting the methods of surveillance to the constraints imposed by the expansion of means of communication ensuring a high level of confidentiality.

In this respect, it should be noted that the first request for **interceptions transmitted or received through satellite**, based on the new provisions of Article L. 852-3 of the French Internal Security Code introduced by law no. 2021-998 of 30 July 2021 on the prevention of terrorist acts and intelligence[19], was submitted in the course of 2024 (see box below).

19. See article 13 of the law introducing a trial period until 31 July 2025.

SATELLITE INTERCEPTION: IMPLEMENTATION OF THE TRIAL PERIOD

Law no. 2021-998 of 30 July 2021 on the prevention of terrorist acts and intelligence, known as the PATR law, introduced a new Article L. 852-3 allowing, for the purposes mentioned in its Article L. 811-3(1) (2) (4) and (6), to use an apparatus or technical device to intercept correspondence sent or received by satellite, "when such interception cannot be implemented on the basis of section I of Article L. 852-1", i.e. when telephone tapping is not possible for operational or confidentiality reasons.

Article 13 of the Act of 30 July 2021 stipulates that these provisions will apply until 31 July 2025 and that the government will submit an evaluation report on the application of these provisions to Parliament no later than six months before this deadline.

As with the security interceptions provided for under Article L. 852-1 of the French Internal Security Code, satellite interceptions are subject to the quota system. However, as no maximum number of authorisations could be granted simultaneously, this new technique was not implemented until 2023.

Progress in the testing phases led to the commission being consulted in 2024 on a proposal to set the quota applicable to satellite-based security interceptions.

In a classified deliberation, the CNCTR considered the government's proposal to set this quota at 20 simultaneous authorisations to be justified and appropriate for continuing the trial under operational conditions.

In practice, one authorisation was issued during 2024.

The bill aimed at freeing France from the trap of drug trafficking, adopted by the Senate on 28 April 2025 and by the National Assembly on 29 April 2025, includes Article 8 *bis*, which extends the trial period until 31 December 2028[20].

20. Based on the numbering in the text adopted on 28 and 29 April by the Senate and the National Assembly. The text was the subject of three referrals to the Constitutional Council on 12 May 2025 (2025-885 DC). The Constitutional Council's decision had not arrived by the date this report was finalised.

1.2.3. A stagnation in the number of authorisation requests for the surveillance of international electronic communications

The CNCTR issued 3,942 opinions in 2024 on requests to **exploit international communications** compared with 3,981 in 2023. Thus, after a slight increase in this number of opinions in 2023 (+7%), a stagnation (-1%) was observed over the past year.

	2020	2021	2022	2023	2024	2023/2024 change	2020/2024 change
Number of opinions issued on the surveillance of international electronic communications	**4,316**	**4,374**	**3,715**	**3,981**	**3,942**	**-1%**	**-8.7%**

LEGAL FRAMEWORK FOR INTERNATIONAL SURVEILLANCE

Surveillance of international electronic communications is governed by the provisions of Articles L. 854-1 to L. 854-9 of the French Internal Security Code. These provide that specialised intelligence services may be authorised to exploit communications emitted or received abroad, intercepted on electronic communications networks designated by the Prime Minister.

These "exploitation" authorisations are issued by the Prime Minister, after consulting the CNCTR. Several categories of authorisation are provided for, depending on the purpose and scope of the surveillance envisaged. This may involve monitoring communications sent or received within a geographical area, by an organisation, by a group of people or by a single individual.

Whatever their nature, these exploitation authorisations may only be based on the purposes listed in Article L. 811-3 of the French Internal Security Code applicable to domestic surveillance.

Subject to exceptions expressly provided for by law, individual surveillance of communications of persons using "national" numbers or identifiers (i.e. "French" communications is prohibited. If such communications are intercepted, they must be destroyed immediately.

1.2.4. A significant increase in requests for additional information made to the intelligence services, leading to a stabilisation in the rate of unfavourable opinions

The progress made by the intelligence services in understanding the legal framework must be seen in the context of a **significant increase in the number of requests for additional information sent by the commission to the intelligence services**. Indeed, these requests, taking all intelligence-gathering techniques together, have increased from 2.9% of the total number of requests in 2023 (2,797 requests for additional information) to 3.3% of the total number of requests for 2024 (3,307 requests for additional information), i.e. an increase of 18.2% in requests for additional information between 2023 and 2024.

Requests for additional information provide an opportunity for exchange between the commission and the intelligence services, and promote a better understanding of the legal framework and the CNCTR's expectations by the latter.

Thus, despite an **increase in the number of requests for intelligence-gathering techniques** made to the commission, this has **not led to a significant increase in the number of negative opinions issued by the commission**.

In 2024, as in 2023, this rate was 0.8% for all techniques combined (775 negative opinions in 2023 compared with 803 in 2024).

If we subtract the opinions issued on requests for internet connection data, the rate of negative opinions increases very slightly from 1.2% to 1.3%. The number of negative opinions thus increased by 9.3% in 2024 compared with 2023, while over the same period requests, excluding internet connection data, increased by just under 5%.

	2023	2024	2023 / 2024 change
Intelligence-gathering techniques (excluding technical connection data)			
Opinions delivered	**39,815**	**41,778**	**4.9%**
Requests for additional information	**1,373** (3.4% of the total)	**1,609** (3.9% of the total)	**+17.2%** (0.5 pt)
Unfavourable opinions	**496** (1.2% of the total)	**542** (1.3% of the total)	**+9.3%** (0.1 pt)
Technical connection data			
Opinions delivered	**55,087**	**57,105**	**3.7%**
Requests for additional information	**1,424** (2.6% of the total)	**1,698** (3% of the total)	**+19.2%** (0.4 pt)
Unfavourable opinions	**279** (0.5% of the total)	**261** (0.5% of the total)	**-6.5%** (0 pt)
All intelligence-gathering techniques combined			
Opinions delivered	**94,902**	**98,883**	**4.2%**
Requests for additional information	**2,797** (2.9% of the total)	**3,307** (3.3% of the total)	**+18.2%** (0.4 pt)
Unfavourable opinions	**775** (0.8% of the total)	**803** (0.8% of the total)	**+3.6%** (0 pt)

At the same time, the context of the Olympic and Paralympic Games and the subsequent mobilisation of the services to prevent threats to the event provided an opportunity for the commission to strengthen a practice introduced in recent years on certain topics. This practice involves asking the services to present their technical surveillance strategy to the board: the intended objective, the choice of targets, and the techniques used. These exchanges are beneficial for both the commission and the services. From the commission's perspective, they allow for a better understanding of the service's approach and help place its requests in the broader context of monitoring an individual or a particular theme. These exchanges are also an opportunity to alert services to the possible

legal fragility of requests that may not be sufficiently well-founded even before they are submitted. For the services, these exchanges help them to understand the commission's expectations and strengthen their ability to submit requests based on solid evidence. The commission intends to continue and deepen these constructive exchanges in 2025.

1.3. The breakdown of requests for intelligence-gathering techniques by purpose remains very similar to that observed in previous years, despite an increase in the number of requests motivated by the prevention of terrorism

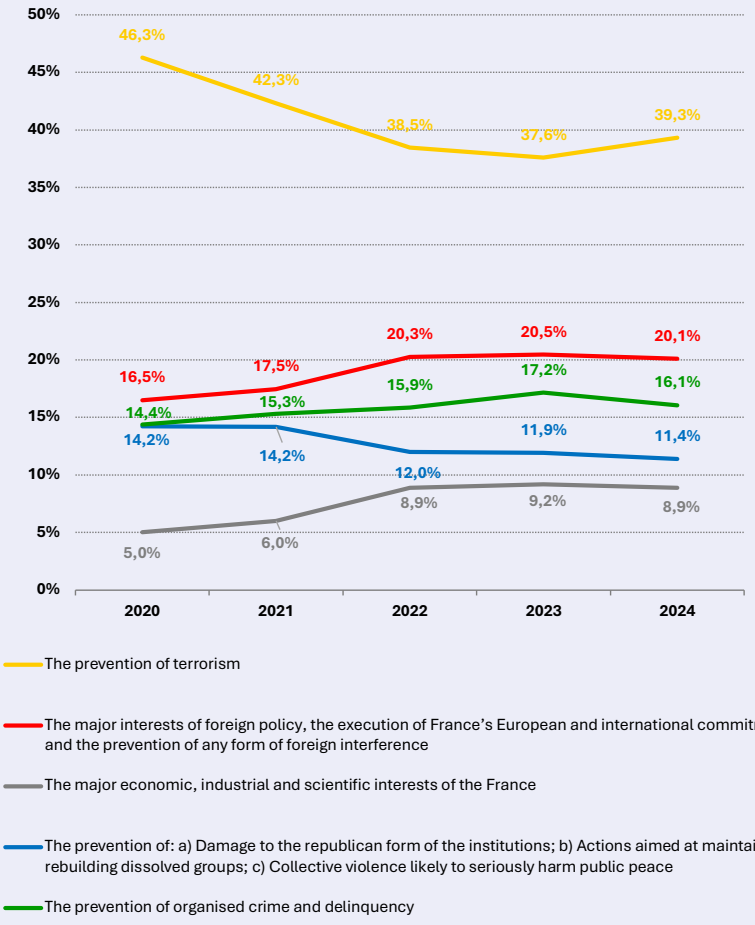
As has been pointed out on several occasions in the commission's previous activity reports, intelligence-gathering techniques may only be used to defend or promote the fundamental interests of the nation, which are listed exhaustively in Article L. 811-3 of the French Internal Security Code.

Although since the creation of the CNCTR, the **prevention of terrorism** has always been the legal basis most frequently invoked in support of requests for techniques, the percentage of requests based on this purpose had nevertheless declined. The year 2024 moderately reversed this trend, as the proportion of requests based on the prevention of terrorism increases by 1.7% compared to the year 2023. Over 39% of requests for intelligence-gathering techniques in 2024 were supported by this legal basis.

The organisation of the Olympic and Paralympic Games appears to be one of the main reasons for this trend, since the risk of terrorist acts of violence was one of the main threats to this event and was therefore a priority for the intelligence services concerned.

However, as in previous years, the terrorist threat remained at a very high level throughout the year.

Number of requests by purpose between 2020 and 2024



As far as the other purposes are concerned, the year 2024 did not lead to any significant changes or developments.

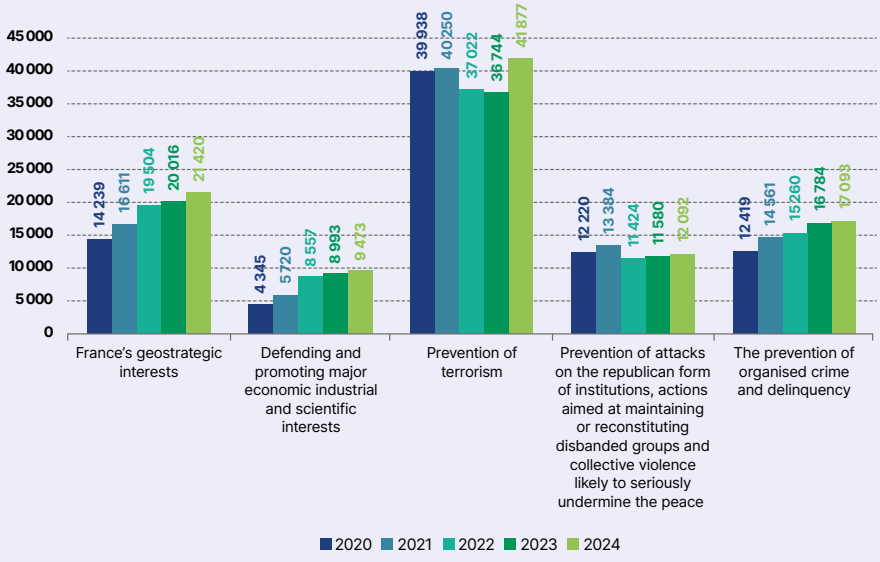
With a ratio of 20.1%, the **purposes relating to France's geostrategic interests** (major interests of foreign policy and prevention of any form of foreign interference) remain the second most frequently invoked legal basis with a stable trend (this ratio was 20.5% in 2023). The services' efforts in these areas have been maintained against a backdrop of growing geopolitical instability.

The share of requests based on the purpose of **preventing organised crime and delinquency** declined in 2024 compared to 2023, from 17.2% to 16.1%. However, it remains by far the third most frequently cited legal basis for requesting the use of intelligence-gathering techniques (this figure is distinct from the number of individuals placed under surveillance on the grounds of this purpose, see point 1.1 above). This slight decline is not the result of a lesser interest on the part of the services in this purpose, but of the slightly greater share taken up by the purpose relating to the prevention of terrorism in the particular context of the year 2024.

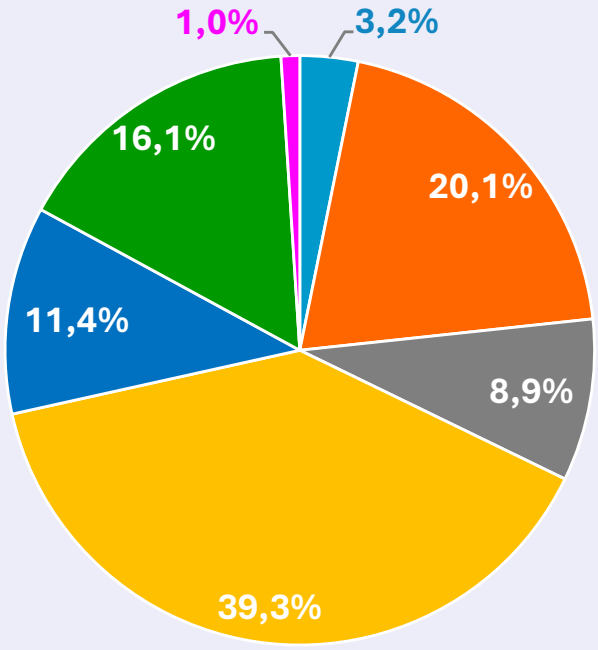
Furthermore, despite a domestic political situation marked by instability and significant tensions in the overseas territories (violent riots in New Caledonia, protest movements in the French West Indies), as well as widespread opposition to major events or certain projects (the organisation of the Olympic and Paralympic Games, the construction of the A69 motorway, large-scale water reservoir projects, etc.), the share of requests based, among other things, on the **prevention of collective violence** continued to decline, standing at 11.4% in 2024 compared to 11.9% in 2023. The number of requests invoking this purpose is nevertheless up very slightly, with around 300 more requests than the previous year.

Finally, the share of the purpose aimed at defending and promoting major industrial and scientific economic interests has stabilised at 8.9% in 2024, compared with 9.2% in 2023.

Number of requests by purpose between 2020 and 2024



Breakdown of purposes underlying all requests for intelligence-gathering techniques in 2024



- National independence, territorial integrity and national defence
- The major interests of foreign policy, the execution of France's European and international commitments and the prevention of any form of foreign interference
- The major economic, industrial and scientific interests of the France
- The prevention of terrorism
- The prevention of: a) Damage to the republican form of the institutions; b) Actions aimed at maintaining or rebuilding dissolved groups; c) Collective violence likely to seriously harm public peace
- The prevention of organised crime and delinquency
- The prevention of the proliferation of weapons of mass destruction

Part 2. Oversight of the use of intelligence-gathering techniques in 2024: many challenges and a mixed picture

As highlighted in the commission's previous activity reports, the ex-post control of the intelligence services' activities serves a threefold objective.

Firstly, it aims to understand the process by which data is collected through intelligence-gathering techniques and the conditions under which that data is used.

Secondly, it aims to verify the lawful use of this data, with particular attention given to situations involving protected professions within the meaning of Articles L. 821-7 and L. 854-3 of the French Internal Security Code (CSI).

Lastly, controls also have an informative, educational and relational dimension, enabling a better understanding of the missions and issues of the intelligence services and their practical implementation by being in contact with operational staff in particular, but also to clear up any misunderstandings that may arise.

In order to maintain and strengthen the credibility and effectiveness of these controls, the commission has for several years been ensuring that its controls are selective and that any anomalies identified are followed up.

However, achieving these objectives requires expertise and resources that match the growing use of increasingly intrusive intelligence-gathering techniques, which allow for the collection of large volumes of highly diverse data, the use of increasingly sophisticated systems for the pre-processing and processing of this data, and the complexity and variety of storage conditions.

In this context, in 2024, the CNCTR faced several challenges in maintaining an effective and credible level and approach to oversight (2.1). While, as in previous years, the commission's assessment of its relationship with the services in this regard remains positive, it regrets the persistence of certain types of anomalies. (2.2). Furthermore, while citizen-initiated oversight continues to progress, it has so far resulted in very few legal challenges before the Council of State and only marginally addresses international surveillance measures (2.3).

2.1. Ex-post control in 2024: the challenge of maintaining effective and credible control

2.1.1. The need to adapt both the scale and methods of oversight in an exceptional context

In 2023, changes in the way controls were organised and carried out, as well as an increase in the number of staff, enabled the CNCTR to carry out particularly intensive controls on the techniques used by the services, with 136 controls carried out on site. **In 2024, various economic factors led to an adjustment in the volume and methods of these controls**.

The organisation of the Olympic and Paralympic Games and a temporary pressure on the commission's workforce led to a 9% drop

in the number of controls carried out, to 123 controls. However, it should be noted that some of these controls were carried out using new methods. Furthermore, in line with the strategy developed over several years, visits and controls in France and overseas were maintained, in favour of a constructive dialogue with the services. Although these figures are lower than last year's, they still reflect a consistently high level of ex-post control activity, exceeding the number of inspections carried out in 2019, 2021 and 2022[21], and with a more targeted approach.

An unavoidable reduction in the number of visits to services in the context of the organisation of the Olympic and Paralympic Games and temporary pressures on the commission's staffing levels

Following prior discussions with the services concerned and taking into account the exceptional mobilisation required of them, the CNCTR has decided, for the period from May to September 2024, to adjust its visits to the services, especially those most directly mobilised by the organisation of the Olympic and Paralympic Games, or to direct its controls so as to involve fewer agents or agents less directly concerned by the management of threats related to this event. So-called data checks, involving checks on the services' IT tools, were less affected. The commission's pragmatic stance was subject to exceptions when necessary.

This adjustment to the volume of oversight was necessary to strengthen the commission's ex-ante control capacity over the same period, in order to cope with the temporary increase in the number of intelligence-gathering technique requests subject to tight processing deadlines[22].

21. Around one hundred controls had been carried out in 2019, 117 in 2021 and 121 in 2022 (the year 2020 had only allowed 76 to be carried out in the services in the context of the health crisis linked to the COVID-19 epidemic).

22. From May to September 2024, the number of commission staff specifically assigned to the ex-ante control mission was increased, notably to handle the rise in requests submitted to the commission within the deadlines set by the French Internal Security Code; 24 or 72 hours depending on the type of request. This team was expanded from 3 to 4 people, then from 3 to 5 people, out of a theoretical total of 14 mission officers.

Finally, **the commission also had to contend, on a temporary basis, with both a significant decrease in its actual number of mission officers** (ranging from -21% to -29%, particularly between September and December 2024) and **a major renewal of its staff**.

These constraints led to 113 controls being carried out directly within the services, to which must be added 10 in-depth remote controls (see below), giving a total of 123 controls. This slight decrease compared to 2023 should not overshadow all the interactions with the services, notably through presentations before the board, questions concerning their practices, or exchanges with the technical departments, which are less easily quantifiable but contribute significantly to the CNCTR's ex-post control mission.

Controls maintained in mainland France and the French overseas territories

In 2024, the commission maintained its visits to the GIC's operational centres across French territory, including the overseas territories, as well as to certain regional branches of the intelligence services, in order to carry out thorough on-site and documentary inspections[23]. Although logistically demanding, these visits have a strong educational component aimed at territorial entities and staff who do not always have the same resources as central departments.

As the commission has explained in its previous reports, **these visits** are used in particular to **meet the local heads of the services** and discuss with them the state of the threat they face at local level and the difficulties they encounter in applying the legal framework. In some cases, particularly in overseas France, they also provide an opportunity to meet with local administrative authorities and judicial representatives.

23. On this point, see the CNCTR's 8th activity report for 2023, p. 51 et seq.

These visits are prepared in advance, covering all the technical monitoring carried out by the services in the area. Beforehand, the services are also encouraged to inform the commission of the issues they wish to raise and the legal and technical questions they have.

In total, **the commission carried out eleven controls and visits to the territories in 2024**, compared with fifteen in 2023. These visits focused on GIC operating centres that the commission had not visited for several years, as well as centres where the volumes of active techniques are more modest, i.e. where local services make less use of intelligence-gathering techniques, in order to ensure that this more sporadic use is not to the detriment of strict compliance with the legal framework.

Emphasis on remote control

In 2024, drawing on its direct access to certain collected data and how that data is exploited, the commission significantly expanded its remote monitoring of the outputs it produces daily as part of its ex-ante control mission and the preparation of all documentary and on-site inspections. It also substantially strengthened oversight of outputs derived from techniques used against protected professions or communications between a surveillance target and a person exercising a protected profession (see point 2.1.2 of this report).

Finally, **the commission developed a specific methodology**, based on a set of specifications drawn up collectively, to carry out in-depth remote inspections, either on cross-cutting themes or on individual surveillance cases likely to raise concerns regarding compliance with legal requirements.

The ex-post control division thus carried out ten in-depth thematic or cross-cutting inspections.

Although highly time-consuming in practice, the commission draws a very positive initial assessment of this new type of remote inspection, which has made it possible to reach well-informed conclusions on various topics and, in some cases, has led to requests for the destruction of collected information.

OVERSIGHT ALSO MEANS SUPPORTING, COMMUNICATING, AND ENGAGING

The commission's oversight mission is not limited to verifying compliance with the legal framework set by the French Internal Security Code. For several years, the commission has also been engaged in explaining the legal framework and sharing its doctrine with the services. This approach takes several forms.

Visits to the services

Whether these visits are strictly for inspection purposes or involve trips to GIC operational centres or local offices of the services, direct exchanges with service personnel provide an opportunity to explain certain opinions issued by the commission, as well as, where applicable, doctrinal positions adopted by the board. The services may also use these meetings to inform the commission of legal difficulties they encounter. These visits serve as a way for the services and the CNCTR to develop mutual understanding, ultimately contributing to better application of the legal framework. It is sometimes observed that the commission and its mission are still not well known among the local levels of the services. It is therefore essential to explain these aspects and to promote knowledge and compliance with the legal framework across all services, wherever they may be.

Contributing to the training of service agents

For several years, the commission has played an active role in training intelligence service agents, as well as senior officials from their supervising ministries, to enhance understanding of the legal framework governing intelligence-gathering techniques, notably through the training programmes provided by the Intelligence Academy[24].

Disseminating the doctrine to the services

After systematising the compilation of its classified doctrine, consolidating it, and carrying out an initial distribution to the intelligence services concerning requests related to the prevention of violent extremism, the commission introduced, at the beginning of 2024, a more regular dissemination process, which takes the form of alert notices and a "newsletter" addressing various issues relating to the application of the legal framework, as examined by the board. The first of these newsletters, sent to the services in March 2024, summarised and explained the key developments in the commission's doctrine during 2023. The second, sent in October, focused on requests concerning protected professions.

2.1.2. | Mixed developments in practical control arrangements

Although there were several improvements in 2024 in terms of the commission's access to certain thematic or technical information, the controls on certain techniques remain uncertain. To fully understand the difficulties, a reminder of the legal rules is in order.

24. On the contribution of the commission to various training courses, see the appendix to this report devoted to the external relations of the commission p. 191 - 3. External relations.

WHAT ACCESS TO DATA DOES THE CNCTR HAVE? PERMANENT, FULL AND DIRECT ACCESS / IMMEDIATE ACCESS / REMOTE ACCESS CONTROL ISSUES

What the law provides for: less access to data by the commission for the techniques that are most invasive of privacy.

The law grants the CNCTR a right of "***permanent, direct and complete***"[25] access to traceability records and to all intelligence derived from intelligence-gathering techniques, whether it concerns collected data or stored information (such as transcriptions and extractions). When the techniques target persons exercising a protected profession , Article L. 821-7 of the French Internal Security Code provides, in addition, that "*transcripts of the information collected [...] shall be transmitted to the commission, which shall ensure the necessary and proportionate nature of any infringements of the safeguards attached to the exercise of these professional activities or mandates*".

Immediate access, which enables the commission to access, from its premises, data as stored in the services' IT systems, is only provided for on a case-by-case basis by law. This is the case with regard to technical connection data collected off-line (Article L.851-1 of the French Internal Security Code) and to transcriptions and extractions resulting from security interceptions whether they are transmitted via electronic communications (Article L. 852-1, V.), by proximity device (Article L. 852-1, I.), or by satellite (Article L. 852-3). The most intrusive techniques are therefore not affected.

25. Article L. 833-2 of the French Internal Security Code provides that: "For the fulfilment of its missions, the commission: [...] 2. Has permanent, complete and direct access to records, registers, collected information, transcriptions, extractions and transmissions mentioned in this book, to the traceability systems for the collected intelligence, and to the premises where this intelligence is centralised under Article L. 822-1, as well as to the intelligence mentioned in III of Article L. 822-2". Article L. 822-1 provides that: "*The Prime Minister shall organise the traceability of the execution of authorised techniques under Chapter I of this title and shall define the conditions for centralising the information collected. To this end, a record is kept of each use of an intelligence-gathering technique. It shall mention the start and end dates of this implementation as well as the nature of the information collected. This record shall be made available to the commission, which shall have permanent, full and direct access to it, regardless of its degree of completion.*"

In certain cases, the law requires the mandatory centralisation of collected and/or stored data within the GIC's information systems. This is the case, for example, with security interceptions carried out via electronic communications, for which section I Article L. 852 of the French Internal Security Code provides for the commission's immediate access to extractions and transcriptions, along with the mandatory centralisation of these operations within the GIC. The same applies to the algorithm-based technique (Article L. 851-3) and real-time geolocation (Article L. 851-4[26]).

The way forward: remote access as a means of guaranteeing "full and direct access" to data.

Rather than advocating for a generalised right to immediate access set out in law, the CNCTR is in favour of any measure that enables **remote access to data from its premises**, as this appears to be, in the absence of immediate access, the only effective way to ensure that it has full and direct access to the data.

By way of illustration, when a security interception is authorised, the centralisation of its execution by the GIC, responsible for forwarding the requests to operators, the mandatory data exploitation carried out under its supervision, and the commission's remote access to the collected data and outputs, together guarantee complete visibility over how the techniques are implemented and how the collected data is used. This arrangement ensures that no data is illegally retained in breach of the authorisation granted, and that no data is subject to improper exploitation by a service.

When the law does not provide for the mandatory centralisation of the use of the technique by the GIC, or for immediate access by the commission, as is the case in particular with particularly intrusive techniques for recording images, words or computer data, two scenarios coexist. Some services have their own centralisation

26. More specifically, Article L. 851-4 of the French Internal Security Code does not expressly state that the GTR (real-time technical data collection) technique is carried out by the GIC, but that the data is transmitted "*to a service under the authority of the Prime Minister*".

solutions, while other services have the option of centralising data using tools offered by the GIC.

Where techniques are not centralised at the GIC, the commission accesses the data by visiting the service's premises and consulting its operating systems. By virtue of its right of direct and immediate access, the CNCTR should in principle have direct access to all extractions and transcriptions made. However, the commission regularly notes the absence of intelligence reports (or exploitation reports, i.e. reports on the information obtained from the use of the intelligence-gathering technique) relating to a technique that is nevertheless presented as effective by the services, and the late preparation of these intelligence reports, sometimes several months after the expiry of the retention period for the data collected, or the presence of data stored on the individual workstations of certain agents, with no obvious traceability, or the existence of tools specific to the service allowing a form of data retention outside of an information bulletin (see point 2.2 of this report, on the anomalies observed).

These findings raise questions about the actual direct and complete nature of the CNCTR's access and reinforce the need to implement the planned remote access to data collected through collection and recording of computer data (RDI) (see point 3.3 of this report). Such remote access would improve the commission's ability to access data and, in parallel, ensure, as required, the lawfulness of the services' actions during both the exploitation and retention (capitalisation) of that data.

The implementation of specific controls and the enhancement of technical and thematic knowledge

Generally speaking, in order to improve its knowledge of specific topics and to better assess the value of certain types of surveillance, the commission has significantly increased its requests to intelligence services for thematic notes or any information document on targets monitored in complex cases, as well as its requests for presentations to the college, on its premises or by

secure videoconference. These exchanges are beneficial for both the commission and the services. From the commission's perspective, they allow for a better understanding of the service's approach and help place its requests for techniques in the broader context of monitoring an individual or a particular theme. These discussions also provide an opportunity to alert the services to the potential legal fragility of requests that may not be sufficiently well-founded even before they are submitted. Furthermore, from the services' perspective, these exchanges help them to understand the commission's expectations and enhance their effectiveness by enabling them to avoid negative opinions in cases where the intended requests lack a valid legal basis. The commission intends to continue and deepen these constructive exchanges in 2025.

With regard more specifically to the supervision of protected professions, applying the provisions of the 4th paragraph of Article L. 821-7 of the French Internal Security Code[27], the commission now requests that all transcripts and extractions made using non-centralised techniques (see box above) implemented against persons exercising a protected activity or mandate within the meaning of this article be presented to it at each control.

Furthermore, a specific reporting procedure has been established, in consultation with the GIC, for certain outputs concerning individuals granted special legal protection, derived from the exploitation of security interceptions. Thus, in pre-identified cases, or at the initiative of the GIC, this the latter forwards to the commission draft transcripts raising a particular difficulty in terms of assessing whether the elements exploited are detachable from the protected activity or mandate. In accordance with the law, no element that can be linked to the profession or mandate may be

27. This paragraph provides that "*transcripts of information collected pursuant to this article [article L. 821-7 of the French Internal Security Code] are transmitted to the commission, which shall ensure that any infringements of the safeguards attached to the exercise of these professional activities or mandates are necessary and proportionate*".

retained or used. The commission's opinion may lead to the deletion of certain outputs or, on the contrary, allow them to be retained, where appropriate, after in-depth discussion with the service.

With regard to the commission's technical knowledge, regular exchanges with the technical departments of certain services in the first circle of the intelligence-gathering community continued throughout 2024. Generally speaking, the commission has initiated a more comprehensive approach with several services to understanding anomalies identified during controls. In addition to exchanges directly linked to the detection and correction of anomalies identified during controls carried out within these services, this technical dialogue aims to identify the causes of persistent irregularities in a more transversal manner and to discuss the adjustments and corrective measures to be taken, in order to prevent their recurrence.

Data access arrangements still imperfect

The year 2024 confirmed that the commission's access to raw data and the results of exploitation, under conditions and in formats that enable it to carry out effective and efficient controls, whether from its own premises or from the premises of the services, remained highly random.

While the commission's remote access to data resulting from the implementation of techniques entrusted to the GIC is satisfactory and was a particular focus of the commission's work in 2024 (see point 2.1.1 of this report), the situation remains mixed in other cases.

In its previous reports, the commission welcomed the increase in technical solutions enabling it to access, from its own premises, the data, transcriptions, and extractions resulting from image and audio recording techniques, and more recently, certain data

obtained through computer data collection by second-circle services, as well as the raw data from mixed communications intercepted under the framework of international surveillance.

However, their use for controls is not yet fully effective. Solutions for centralising data from image and voice recording are not widely deployed in France, or do not have sufficient bandwidth, so they are rarely used by the services. Similarly, the tool for centralising data from certain RDIs at the GIC is very little used; the difficulties encountered by the services in exploiting the data do not encourage them to use it (see section 3.3 of this report). Lastly, the commission has, in practice, been deprived for several months of effective access to raw data from mixed communications. To date, the CNCTR has not received any concordant explanation of the reasons for this interruption of access.

As regards non-centralised techniques for which the data can only be accessed on the premises of certain services in the first circle, the commission's access remains random, despite the fact that these are some of the most intrusive techniques, within the services that use them the most.

First of all, the commission would point out that these controls, which involve agents going on site at pre-established times, necessarily have a limited scope in quantitative terms, as the number of techniques that can actually be controlled is extremely small compared to the number of authorised techniques.

The commission is also regularly confronted with problems of access to data in the context of these controls.

By way of illustration, regarding the raw data collected through the use of IMSI catchers, the commission faced several months of deteriorated access within a major service. While it had previously benefited from access under conditions equivalent to

those of the service's operational staff, it was subsequently deprived of the tools necessary to interpret that raw data. Access has now been restored under satisfactory conditions.

With regard to access to data from computerised data collections, the commission has had to deal with a number of cases that highlight the dependence of its controls on the availability and proper functioning of the tools made available by the services.

In one service, for example, an error in the allocation of IT rights to the commission's agents prevented access to data from the RDIs for several months. In another service, the obsolescence of the IT hardware made available to the commission meant that it was very difficult to open files from RDIs, and the controls were rarely successful. In the summer of 2024, the service replaced all the computer workstations dedicated to the commission's controls.

Although on each occasion the services concerned took the necessary steps to resolve the problems once the cause had been identified, this is a matter for the commission to be vigilant about; the effectiveness, and consequently the credibility, of its controls is not a foregone conclusion.

Some of the progress announced has not yet been achieved. By way of illustration, as part of the discussions on the project to centralise all computer data collection techniques (see the 2023 activity report and section 3 of this report), a first-circle service, which is particularly concerned by this issue, had committed, pending the implementation of this project, to establishing a procedure for directly transmitting part of its transcriptions to the commission, under conditions still to be defined. However, the implementation of this commitment, which was due to take place after the Olympic Games period, is still not in effect. The commission will work with the service to ensure that this transmission process is properly implemented during 2025.

With regard to the oversight of international surveillance measures, while the commission welcomes having had access, since the beginning of 2024, to a dedicated room for monitoring the six services authorised to use such measures, it regrets that it still does not have access to the same tools as those used by the staff of these services. Moreover, the commission regularly faces logistical difficulties: including conditions of access to the premises and data, the functioning of the equipment provided, and the ergonomics and speed of the oversight tools, all of which undermine the effectiveness of the oversight process and the ability of the commission's staff to build expertise.

2.2. Oversight findings: anomalies of varying severity, but their persistence raises concerns

The number of anomalies identified in 2024 is comparable to previous years. Their detection systematically led to exchanges with the intelligence services, which took steps to resolve them within a reasonable timeframe, without the commission having to resort to the formal recommendation power granted to it under Article L. 833 6 of the French Internal Security Code. The committee welcomes this.

As a preliminary point, however, the commission recalls that its ex-post control of the data collected and retained by the services can, by definition, only be carried out on a sampling basis and, in practice, covers only a very small proportion of all data resulting from the intelligence-gathering techniques implemented. However, almost all the data checks carried out under so-called domestic or international surveillance lead to the discovery of persistent anomalies of varying degrees of seriousness, which leads the commission, after ten years of carrying out its ex-post controls,

to consider that the number of anomalies actually discovered can only very partially reflect reality.

This finding has prompted the commission, in consultation with the services most concerned, to develop a more global approach to identifying the most recurrent anomalies, their causes and the corrective measures to be taken (see point 2.1.2 of this report).

Finally, in order to provide a better understanding of the scope of the anomalies observed, this year's report is supplemented by two inserts explaining the particular challenge of correctly completing traceability sheets and intelligence reports (or operating reports).

2.2.1. | Anomalies identified at the data collection stage

As in the previous year, irregularities relating to the conditions and procedures for the implementation of techniques: scope, duration of authorisation, target person, were noted. Although they were less frequent than those relating to the use of the techniques, they were much more serious because they lead to the collection of data that should not have been collected, or at least under conditions that were not provided for in the authorisation given after the commission's opinion. All the irregularities observed were notified to the services concerned, who undertook the requested deletions and corrections.

Several "typical" scenarios are encountered.

Certain restrictions concerning how intelligence-gathering techniques are implemented, which the commission explicitly states in its opinions, are not respected. Yet these restrictions are specifically intended to limit the extent of the intrusion into the privacy of the person under surveillance or third parties. In other words, they enable the commission to ensure that any interference

with privacy is proportionate to the threat posed by each individual concerned. As in the previous year, the failings noted again in 2024 concerned the technique of computer data collection, which covers very different methods of implementation, the intrusiveness of which varies greatly. The services concerned have changed their practices and tools to ensure that the restrictions imposed by the commission are effectively taken into account.

In this respect, the commission calls on the services to be particularly vigilant in taking account of its opinions containing restrictions.

Data was collected when the authorisation for implementation had expired. In one case, the use of a technique during a so-called "gap period" appeared to be all the more problematic as the traceability sheet filled in by the service was incorrect as it stated that the intelligence-gathering techniques had been deactivated. However, the controls concluded that the service had not acted in bad faith. The data was destroyed and the traceability modified at the request of the commission. However, the attention of the services should be drawn to the need to set up an internal system, firstly organisational and if possible technical, to ensure that the deadline for authorising the use of the technique is systematically respected, by all levels involved in the implementation of the technique.

Anomalies relating to the exceeding of the object of surveillance have again been noted. These are cases where a service continues to implement a technique even though the person under surveillance is not or is no longer present in the location specifically covered by the authorisation. This is generally due to a difficulty in setting the parameters of the recording device and to operational constraints linked to the specific nature of certain places which do not allow officers to intervene immediately in order to limit the use of the technique to what is strictly necessary. The commission urges all services that may be concerned to put in place an internal procedure for detecting and deleting data collected in this way as quickly as possible.

Two more atypical cases can also be mentioned.

The first concerned a particularly atypical use of the technique of recording images in a private place. The service, considering that the latter did not fall within the scope of Article L. 853-1 of the French Internal Security Code, had not requested authorisation for its implementation. The commission nevertheless considered that the techniques implemented should have been authorised on the basis of Articles L. 853-2 and L. 853-3 of the French Internal Security Code and notified the services, which indicated that they had removed the equipment and deleted the data collected.

The second case highlighted a failure by a service to carry out the necessary checks to detect whether the person under surveillance was practising a protected profession.

The scenario of unexpectedly discovering, during the exploitation of a technique, that the person concerned holds a protected mandate or exercises a protected profession has already been encountered and does not, in itself, constitute an irregularity. While such situations cannot be entirely ruled out, the services are nevertheless responsible for carrying out the necessary investigations to minimise the likelihood of this occurring. In the case at hand, the service had requested authorisations to implement intelligence-gathering techniques targeting individuals whose identities, and therefore their professions, were still unknown at the time the request was processed. However, the service had provided assurances that it would carry out the necessary checks to establish those identities as soon as possible and, in any event, before the techniques were implemented. The commission, which noted that these checks had not been carried out when the services informed it, on their own initiative, of the discovery of the profession exercised by the persons concerned, requested that the data be destroyed. These irregularities were also the subject of a letter from the CNCTR chairman to the director of the service.

2.2.2. Anomalies identified in the traceability of the implementation of intelligence-gathering techniques

Recurring shortcomings in the preparation and transmission of implementation records, known as "traceability sheets", were once again noted in 2024.

Without proper traceability, the commission cannot know whether an authorised technique was actually implemented, or under what conditions. This limits its ability to prepare ex-post controls effectively, but above all to detect any anomalies and, where necessary, to examine requests for renewal of the techniques concerned in an informed manner. The commission therefore regularly encourages services to be rigorous in drawing up traceability sheets, even when the technique has not been used.

In addition, on two occasions in 2024, more specific steps were taken in this area. On the one hand, this concerned a service for which the commission had repeatedly noted that traceability sheets were either not completed, completed very late, or lacked sufficient detail, despite the service having made significant efforts on this issue in previous years. Commitments have been made to improve these practices, but they will need to be verified over the course of 2025. On the other hand, the issue involved a service being asked to provide more detailed traceability for the implementation of audio surveillance techniques, which required the deployment of several technical devices, as well as for computer data collection. The service concerned promptly implemented the requested changes.

WHAT IS THE PURPOSE OF A TRACEABILITY SHEET?

Under the terms of Article L. 822-1 of the French Internal Security Code, a statement of implementation of each intelligence-gathering technique, mentioning "*the start and end dates of implementation as well as the nature of the information collected", shall be established. This statement, more commonly referred to as a "traceability sheet*", is "made available to the commission, which shall have permanent, full and direct access to it, regardless of its degree of completion".

Article L. 833-2(2) of the French Internal Security Code provides that the commission "*has permanent, complete and direct access to records, registers, collected information, transcriptions, extractions and transmissions mentioned in this book, to the traceability systems for the collected intelligence, and to the premises where this intelligence is centralised under Article L. 822-1, as well as to the intelligence mentioned in III of Article L. 822-1*".

In practice, traceability sheets are transmitted to the commission *via* the intelligence-gathering request and validation tool provided by the GIC, which is accessible to the services, the commission, and the Prime Minister from their respective premises. The commission can also consult them directly within the services' information systems during site visits.

Completing these sheets fully and promptly is essential to enable all stakeholders involved in verifying the legality of intelligence-gathering techniques, including internal oversight bodies, to carry out the necessary checks for their respective missions.

First and foremost, the sheets allow the service itself to verify that the implementation conditions comply with the legal framework and the terms of the authorisation. Completing the traceability sheet and the hierarchical checks carried out at the time of validation are steps that are supposed to enable the agent and their superiors to detect any irregularities committed during the implementation of a technique.

The GIC then performs a control of the traceability sheets, checking whether they have been properly transmitted by the services and identifying any discrepancies between the information stated in the authorisation request and the content of the sheet. When an anomaly is detected, the GIC notifies the service concerned and, in the absence of a response, may report the matter to the Prime Minister, who can decide to terminate the technique.

Traceability sheets also enable the CNCTR to access the necessary information to properly assess renewal requests and to detect irregularities even before accessing the data itself, or at the very least, to identify the elements needed to prepare its inspections.

2.2.3. Anomalies identified in the retention and exploitation of data

The recurring, and in some cases structural, nature of anomalies relating to the retention and exploitation of data from certain intelligence-gathering techniques is regularly noted by the commission in its activity reports. The persistence of such anomalies nearly ten years after the Law of 24 July 2015 is regrettable.

The first issue concerns cases where the legal retention period for collected data has been exceeded[28]. These irregularities, which were more numerous than in 2023, mostly involved data obtained through the most intrusive techniques, namely the recording of words and computer data collection.

However, these situations were mainly encountered within a first-circle service that uses its own internal data centralisation system. In such cases, the data falls outside the centralisation

28. The retention periods are set by the provisions of Article L. 822-2, I of the French Internal Security Code.

mechanism organised by the GIC (see the information box concerning the different types of CNCTR access to data on p. 66). As noted in the 2023 activity report, this means that compliance with the rules on data retention and exploitation depends on the reliability of the internal procedures put in place by the services.

In most cases, the irregularities were due to a failure in the service's automatic data deletion script, which led to excessive retention of the raw data collected. Discussions with the service concerned made it possible to identify the issue, which led to the development of technical solutions to resolve the problem that had been causing recurring irregularities. The data was also immediately destroyed by the service.

As for the exploitation of data, the commission monitors the "extractions" and "transcriptions", which correspond to data the service considers "relevant" and which, as such, may be retained for as long as they remain "***strictly necessary for the achievement of the legal purposes***"[29]. As it does every year, the commission identified several cases where transcriptions[30] included content with no clear link to the intended purpose, or even to the person concerned by the technique. Other cases involved the transcription of information inseparable from the protected activity[31] exercised by the person under surveillance or their interlocutor. This type of irregularity, which can be considered "common", leads to exchanges with the service, which may present relevant information ultimately justifying a link with the purpose or the target and, as a result, the retention of the information. If not, the information must be destroyed by the service, which must provide proof of this to the commission.

29. See III of Article L. 822-3 of the French Internal Security Code.

30. These transcripts are recorded in intelligence reports.

31. Within the meaning of Article L. 821-7 of the French Internal Security Code.

Last but not least, it was once again the complete absence of intelligence reports (or "exploitation reports") that caught the commission's attention in 2024[32]. These shortcomings are recurring, especially when the exploitation of techniques is not centralised via the GIC. The commission regularly reminds the services of these requirements, as such shortcomings are particularly problematic.

Indeed, without an intelligence report or where such reports lack certain minimum information, the commission's ability to conduct oversight is severely hampered. However, the anomalies observed in this area most often relate to the most intrusive techniques, due to lower levels of centralisation during their implementation and the commission's more limited access to the data.

The persistence of shortcomings, whether related to incomplete, missing, or delayed transmission of exploitation results, already observed in previous years, led the chairman of the CNCTR to hold more formal discussions with the leadership of one service. That service committed to issuing the necessary reminders to its staff and to implementing internal measures to ensure that intelligence reports are complete, prepared within the required timeframe, and produced using the designated exploitation tools, under conditions that allow the CNCTR full and direct access. Checks carried out in 2025 will determine whether the promised improvements have been effectively implemented.

32. See box below.

SHORTCOMINGS IN INTELLIGENCE REPORTS: CNCTR OVERSIGHT, PRACTICAL CHALLENGES, AND IMPLICATIONS

The "intelligence reports", also referred to as "exploitation reports", "exploitation results", or "outputs", correspond to the "***extracted or transcribed intelligence***", the collection, retention, transmission, and destruction of which are governed by Articles L. 822-3 and L. 822-4 of the French Internal Security Code. Section I of Article L. 822-3 specifically provides that:

"***Intelligence may not be collected, transcribed, extracted, or transmitted for purposes other than those set out in Article L. 811-3***". Section III of the same article further provides that "***transcriptions or extractions must be destroyed as soon as their retention is no longer strictly necessary for the pursuit of the purposes set out in I***".

The law therefore defines "extracted or transcribed intelligence" by its intended purpose. **In practice, this refers to information considered "relevant" with regard to the purposes listed in Article L. 811-3 of the French Internal Security Code**. This link with one or more legal purposes justifies the retention of such intelligence by the service beyond the legal retention period for the collected data, for as long as it remains strictly necessary to pursue those purposes. This is referred to as "retained data".

The oversight actors

The exploitation of intelligence-gathering techniques is first subject to internal oversight within the services themselves, intended to ensure that agents comply with the legal framework.

The GIC, for its part, carries out exhaustive checks on all outputs (transcriptions or extractions) produced by the services concerning those intelligence-gathering techniques for which it centralises exploitation. Each proposed transcription or extraction is therefore subject to verification of the traceability of the implementation of

the relevant technique, the link between the exploited information and the objective stated in the authorisation, as well as the connection between that information and the purposes set out in Article L. 811-3 of the French Internal Security Code. In the case of individuals exercising a protected profession or mandate, the GIC also ensures that the exploited information can be clearly separated from the protected activity. Only outputs validated by the GIC are subsequently transmitted to the services.

When exploitation occurs outside the GIC's information systems, these checks may be carried out through documentary review and on-site inspections, with the GIC having the same level of access as the CNCTR to collected data, traceability systems, and exploitation results.

The CNCTR has access, from its own premises, to all outputs validated by the GIC concerning so-called "centralised" techniques. For the others, the commission carries out on-site inspections at the premises of the intelligence services to conduct its oversight.

The scope of the commission's oversight

Transcription operations are subject to CNCTR oversight.

Article L. 833-2 of the French Internal Security Code specifically provides that: "*For the fulfilment of its missions, the commission: […] 2. Has permanent, complete and direct access to records, registers, collected information, transcriptions, extractions and transmissions mentioned in this book, to the traceability systems for the collected intelligence, and to the premises where this intelligence is centralised under Article L. 822-1, as well as to the intelligence mentioned in III of Article L. 822-2*".

Where these operations concern individuals exercising a protected profession, Article L. 821-7 of the French Internal Security Code further provides that: "*transcripts of the information collected under this article shall be transmitted to the commission, which shall ensure the necessary and proportionate nature of any infringements of the safeguards attached to the exercise of these professional activities or mandates*".

Lastly, under Article L. 833-6 of the French Internal Security Code, "*the commission may, at any time, issue a recommendation to the Prime Minister, the minister responsible for its enforcement, and the relevant service that the implementation of a technique be terminated and the collected intelligence destroyed when it considers that: […] 3. The collection, transcription, extraction, retention, destruction, or transmission of collected intelligence between services has been carried out in breach of Chapter II, Title II of this book*."

The law thus primarily governs the commission's responsibilities with regard to "extracted or transcribed" intelligence in terms of its access arrangements for such intelligence and its powers of recommendation, without precisely defining the scope of its oversight. Article L. 833-6 of the French Internal Security Code refers, in very general terms, to "breaches" of the procedural rules governing the implementation of intelligence-gathering techniques. The scope of the commission's oversight is therefore broad.

In practice, oversight of intelligence reports serves three main purposes.

First, the CNCTR ensures that the services actually produce these intelligence reports and that the commission has direct access to them. More specifically, it checks that the information retained by the services is not stored on systems to which the commission does not have direct access, in breach of the provisions set out in Article L. 833-2 of the French Internal Security Code. It regularly questions the absence of intelligence reports when the technique is nonetheless described as productive by the service, especially when requesting the renewal of authorisation for its use. This absence reveals that, with regard to techniques not "centralised" by the GIC, and despite the development of dedicated information systems for data exploitation it remains common practice for some agents to work with personal, decentralised files, without any traceability and therefore without the possibility of oversight.

When an intelligence report has been prepared, the commission verifies the relevance of the information it contains, which justifies its retention by the service: Is the retained information relevant to the purpose of the surveillance? Does it concern the person targeted by the authorisation? Can the information clearly be separated from any protected profession or mandate exercised by that person?

Lastly, intelligence reports contain several elements, beyond the intelligence itself, that help the commission assess the legality and regularity of the technique's implementation. The very limited number of relevant elements transcribed by the service may, for example, lead the commission to question the continuation of surveillance when it does not appear to produce any useful information, while at the same time genuinely infringing on the privacy of the person concerned. The CNCTR may also question the choice of purpose for which authorisation was granted. It can also detect anomalies linked to the irregular implementation of the technique, for example with regard to the actual place of implementation of the technique or the person supposed to be targeted by the technique.

In this regard, the commission regularly emphasises the need for properly prepared intelligence reports for so-called "non-centralised" techniques, as failure to do so prevents the commission from carrying out its oversight of compliance with the legal framework. A certain amount of information must be included, in particular that which makes it possible to identify the presence of the person concerned when the conversations or images that may have been captured are being used, to determine the date on which the data being used was collected or the methods of collection and the media that may be involved. The commission encourages services to align these reports, as much as possible, with the model for exploitation results available in the GIC tools for "centralised" techniques.

2.2.4. Anomalies identified in the surveillance of international electronic communications[33]

In this area, as in previous years, the commission observed recurring anomalies involving the exploitation and even the retention of national communications.

Anomalies linked to surveillance affecting national territory

In 2024, controls revealed on several occasions, in various services, the retention of connection data collected about a person under surveillance when that person was on national territory or possibly residing there, on the basis of an authorisation to use the international surveillance system, both in the absence of authorised individualised techniques on that person and outside the specific regimes authorising any retention of data in this situation.

This type of anomaly was found in files containing connection data revealing communications located on national territory. With regard to content, on several occasions the CNCTR discovered in intelligence reports summarising information collected under an exploitation authorisation, the retention of successive information despite the apparent presence or residence of the person under surveillance on national territory.

These observations were explained by the services concerned as being the result of errors on the part of the operational agents and stemming from an inadequate understanding of the legal framework, combined with difficulties in systematically controlling the large volume of data collected through the various exploitation authorisations relating to international communications.

33. See the box presenting the legal framework for international surveillance on p. 50 of this report.

In these different situations, the CNCTR verified that its requests for the destruction of data that should not have been retained were properly carried out.

Anomalies relating to protected professions within the meaning of Article L. 854-3 of the French Internal Security Code

Certain anomalies, though more rare, concern cases where, during an ex-post inspection, it is discovered that a person whose data was retained under international surveillance exercises a protected profession or mandate, while being present on national territory. In such cases, the CNCTR requests that the service submit a new request for authorisation to exploit the connection or content data, as applicable, to be examined by the board sitting in plenary session, as required by law, in order to assess whether the information sought can be clearly separated from the protected profession or mandate.

Anomalies relating to the type of data requested by agents

Other anomalies, observed repeatedly, concern the type of data that was searched for and retained by the service, even though the granted exploitation authorisation did not cover that category of data.

Furthermore, the services sometimes access connection data of interest without explicitly mentioning this data in the documents attached to the authorisation request, as required by the legal framework. In the case of a large amount of connection data for a targeted person, the services may have neglected to carry out this referencing work beforehand, leading to a more time-consuming and tedious process of verifying the origin of the data and the reason for its retrieval.

These different types of anomalies can be explained by errors of understanding and, consequently, of application, of the scope of

the authorisations granted concerning the nature of the data to which access is permitted, as well as the extent and accuracy of the information such data provides to the service.

Over the course of 2024, the technical characterisation of the data concerned, the clarification of the scope of the various authorisations provided for in articles L. 854-1 et seq. of the French Internal Security Code and to clarify and disseminate the commission's policy, initiated in previous years, continued in conjunction with the intelligence services in order to prevent this type of anomaly from occurring.

Anomalies linked to the absence of a connection with key components required for the exploitation authorisation

During its inspections, the CNCTR regularly finds that there is sometimes a tenuous link, or even no link at all, between the information collected under an exploitation authorisation and recorded in intelligence reports and the purpose or purposes mentioned in Article L. 811-3 of the French Internal Security Code on the basis of which the authorisation was granted.

This may include a lack of connection to the geographic area covered by the authorisation, searches conducted on an entity that was not listed in the documents associated with the authorisation, or a link that appears insufficient with the purpose under which the authorisation was issued.

The CNCTR is careful to remind the services of the need to adopt a rigorous approach and to pay particular attention to the coherence of the various elements making up an exploitation authorisation throughout its lifecycle, both in its legal formalisation and in the results obtained from its use.

Anomalies linked to the authorised exploitation period

Checks on the use of exploitation authorisations sometimes reveal that information is collected during so-called "gap periods", occurring when the service fails to renew the relevant authorisation before the authorised period expires. There have also been occasional instances of the authorised duration being exceeded, in cases of specific usage regimes and/or poor justification for the various authorised exploitation periods, leading the CNCTR to request the deletion of data collected outside of the authorised period.

2.2.5. Follow-up to findings of anomalies

As in 2023, all the findings and analyses drawn up by the commission during 2024 were the subject of a consensus with the intelligence services, which took care to resolve the anomalies identified within a reasonable timeframe, without the commission having to make use of the power of formal recommendation conferred on it by Article L. 833-6 of the French Internal Security Code, or to issue an unfavourable opinion regarding the renewal of the authorisation concerned by the irregularity.

This year, moreover, **the commission did not have to note any errors in the reports sent by the services following requests for the destruction of collected data or transcriptions**. It welcomes this progress.

Persistent or repeated shortcomings, requiring hierarchical intervention and the ongoing involvement of the services' internal oversight bodies, may lead to a more formal notification by the chairman of the commission to the director of the service concerned. **The commission remains highly attentive to the results of the actions undertaken or announced by the service concerned**.

2.3. Oversight at the initiative of individuals: complaints continue to rise without leading to increased litigation before the Council of State, and without questioning international surveillance measures

The CNCTR may be contacted by any person wishing to verify that no intelligence-gathering technique is or has been unlawfully implemented against them. This prior complaint procedure is provided for under Article L. 833-4 of the French Internal Security Code for so-called domestic techniques, and under Article L. 854-9 of the same code for the surveillance of international electronic communications.

The power of verification thus conferred on the commission relates solely to the intelligence-gathering techniques provided for in the French Internal Security Code and does not therefore extend to surveillance measures ordered by the judicial authority or to those, which are of course illegal, carried out by private individuals.

For reasons of national security, and pursuant to the provisions of Decree No. 2015-1405 of 5 November 2015 on exceptions to the application of users' right to refer matters to the administration electronically, individuals wishing to request verifications concerning themselves may only validly contact the commission by sending a letter by post.

The complaint must be submitted by the person concerned or their legal representative, giving proof of their identity and stating the technical identifiers that they wish to be subject to verification. These technical details, such as telephone numbers or email

addresses, must be supported by documentary evidence, such as a subscription contract or invoice.

Checks can only be carried out once all this information and supporting documents have been sent to the commission. Complete complaints are then examined using the same methods and tools as those applied when the commission carries out ex-post control on its own initiative.

2.3.1. A continued increase in both the number and precision of complaints

While 2023 saw a significant increase in the number of complaints, with annual growth of more than 65%, this growth slowed sharply in 2024. With 87 complaints received in 2024 compared with 81 in 2023, the increase amounts to 7.5%.

	2016	2017	2018	2019	2020	2021	2022	2023	2024
Number of complaints	**49**	**54**	**30**	**47**	**33**	**48**	**49**	**81**	**87**

The year 2024 confirmed a trend already noted in the previous activity report with regard to the completeness of the complaint files received.

Indeed, the proportion of requests that could be processed upon receipt, that is, without asking the complainant to send additional documents, has continued to increase, rising from 18.4% in 2022 to 34.4% in 2023, and to 44.8% in 2024.

In addition, 9 of the complaints received in 2024, i.e. slightly more than 10%, were made by individuals who had already approached the CNCTR for verification in previous years, or, in the case of one of them, during 2024 itself.

Taken together, these factors show that the public is more aware of the existence of the CNCTR and the procedures for referring cases to it.

As in previous years, the response time for complaints containing all the information required to process them was well under two months[34].

No complaint has led the CNCTR to issue a recommendation to the head of the intelligence service concerned, to the minister to whom it reports or to the Prime Minister, requesting that the use of a technique be halted and the information collected destroyed, in accordance with Article L. 833-6 of the French Internal Security Code.

2.3.2. Appeals before the Council of State remain very limited

Articles L. 773-1 et seq. of the French Administrative Justice Code establish a special legal procedure allowing individuals to ask the specialised panel of the Council of State to verify that no intelligence-gathering technique is or has been unlawfully implemented against them. The members and the public rapporteur of the specialised panel are authorised by virtue of their position to have access to information protected by national defence secrecy.

In the case of intelligence-gathering techniques relating to domestic surveillance, the matter may be referred to the specialised panel of the Council of State on the basis of Article L. 841-1 of the French Internal Security Code, by any individual who can prove they have first exercised their right to submit a complaint to the CNCTR.

In the case of surveillance of international electronic communications, only the chairman or at least three members of

34. This period runs from the date on which the complaint can be investigated. Where a request for additional documents (proof of identity, proof of subscription, etc.) has been sent to the complainant, the time limit does not start to run until these documents have been received.

the committee may refer the matter to the Council of State. However, the rules governing domestic surveillance apply if the verification concerns the legality of exploiting communications from individuals using identifiers linked to French territory and communicating from or to France. These individuals may themselves refer the matter to the Council of State after first submitting a complaint to the commission[35].

Seven new applications were registered with the Council of State under Article L. 841-1 of the French Internal Security Code in 2024, compared to five in the previous year, and nine decisions were issued, four of which concerned cases registered in 2023. At 31 December 2024, two cases registered in 2024 remained pending.

The CNCTR is informed of any application filed under Article L. 841-1 of the French Internal Security Code and is invited to submit written or oral observations, where applicable. It therefore has observer status before the Council of State. As the decision-making authority, the Prime Minister, represented by the GIC, is responsible for defending the State.

The CNCTR submitted observations on all applications forwarded to it by the Council of State.

As in previous years, the commission did not find itself in a position to bring an action before the Council of State on the basis of Article L. 833-8 of the French Internal Security Code. This remedy is available to the chairman of the commission or to three of its members when the Prime Minister fails to act, or acts inadequately, on the commission's opinions or recommendations[36].

35. See point 2.3.3 below.

36. The commission was not required to refer the matter to the Council of State under the conditions provided for by the provisions of the second paragraph of Article L. 821 1 of the French Internal Security Code, as amended by the law of 30 July 2021. Pursuant to these provisions, the chairman of the CNCTR or one of its members who is a magistrate must immediately refer the matter to the Council of State when the Prime Minister issues an authorisation to implement an intelligence-gathering technique after receiving a negative opinion from the commission. The Council of State shall then rule within twenty-four hours of the referral. The Prime Minister's authorisation decision may not be implemented before the Council of State has ruled, except in duly justified cases of urgency and if the Prime Minister has ordered its immediate implementation. In 2023, as in previous years, the Prime Minister followed all negative opinions issued by the CNCTR.

2.3.3. No direct referral in matters of international surveillance, while the control procedures in this area have not seen any improvement

In accordance of the provisions of Article L. 854-9 of the French Internal Security Code, any person wishing to verify that no international electronic communications surveillance measure or one-off verification[37] has been or is being unlawfully implemented against them may submit a request to the CNCTR to that effect.

As in the case of domestic surveillance, the commission shall then ensure that any surveillance measures implemented comply with the applicable legal and regulatory framework and with the decisions and authorisations of the Prime Minister. Once the checks have been carried out, it notifies the complainant that these checks have been carried out, without confirming or denying that surveillance or *ad hoc* verification measures have been implemented.

In 2024, one complaint was considered to relate to the verification of the regularity of the implementation of international surveillance measures. When the information brought to its attention in the complaint includes a foreign element, such as foreign identifiers or links to another State, the commission automatically carries out checks in this regard.

However, in line with the observations made by the commission in its previous activity report[38], it should be emphasised that if

37. The Prime Minister's authorisation to exploit communications sent or received abroad, or solely the intercepted connection data, constitutes authorisation to carry out one-off verifications within the intercepted connection data, strictly for the purpose of detecting a threat to the Nation's fundamental interests, linked to relations between subscription numbers or technical identifiers associated with French territory and the geographic areas, organisations, or individuals referred to in point 3 of Article L. 854-2, III of the French Internal Security Code. For the sole purpose of urgently detecting a terrorist threat, this occasional verification may cover communications from subscription numbers or technical identifiers linked to the national territory. One-off checks may also be carried out to detect, for technical analysis purposes, elements of cyberattacks likely to harm the fundamental interests of the Nation on communications of technical identifiers linked to the national territory.

38. See the CNCTR's 8th activity report for 2023, p. 58 et seq.

the complaints referred to it were to relate more frequently to international surveillance measures or contain elements leading it to carry out checks on its own initiative, the practical arrangements for its control in this area would make it very difficult to comply with the two-month time limit within which the complainant may refer the matter to the Council of State.

The lack of remote access to the computer applications used by the services in this area means that checks must be carried out in each of the six specialised intelligence services that may use international electronic communications surveillance measures in order to carry out the necessary verifications, which can be lengthy and complex.

Part 3. Areas for vigilance and outlook for 2025

3.1. The 10 December 2024 decision of the European Court of Human Rights on the applications concerning French legislation on intelligence confirms the role of the CNCTR but leaves several fundamental issues unresolved

As the commission recalled in its previous report[39], twelve applications were lodged with the European Court of Human Rights in 2015 by journalists, lawyers and organisations representing the interests of these professions, followed by two additional applications from journalists in 2017. All of the applicants argued that French legislation on intelligence-gathering techniques, resulting from law no. 2015-912 of 24 July 2015, violated the right to privacy, the right to an effective remedy and the right to a fair trial, guaranteed respectively by Articles 8, 13 and 6§1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The journalists also claimed that their sources had been compromised, and the lawyers claimed that the confidentiality of their communications with their customers had been breached.

After a lengthy investigation, the Court, in a decision of 10 December 2024, made public in January 2025[40], ruled that the various applications were inadmissible, as requested by the French government, on

39. See the CNCTR's 8th activity report for 2023, p. 82 et seq.

40. See ECHR, 10 December 2024, Association confraternelle de la Presse Judiciaire and others, No. 49526/15 and 13 other applications, published on 16 January 2025.

the grounds that the applicants had not exhausted domestic remedies[41]. The 2015 applicants had not asked the CNCTR to ensure that they had not been subject to illegal surveillance[42]. As for the 2017 applicants, they had indeed referred the matter to the commission and then to the Council of State ruling on the dispute, but they had not invoked a violation of the rights guaranteed by the Convention in support of their appeals.

The safeguard mechanism established by the Convention through the creation of the Court is subsidiary to national systems for the protection of human rights[43]. This means that, before bringing a case before the court, the legal remedies available under national law must be exhausted. The court's decision emphasises that this principle is particularly important where national defence secrecy is at stake, since the domestic courts, which have access to the documents covered by that secrecy, are better placed to strike a balance between the interests involved.

However, **this obligation to exhaust domestic remedies is valid only if the remedies provided for by national law are effective**. Before upholding the Government's plea of inadmissibility, the court therefore had to examine in detail the remedies available before the CNCTR and then before the Council of State[44]. Having examined the matter in the light of the criteria laid down in previous judgments[45] and relying in particular on the activity reports of the commission, it concluded that the procedural aspect of **the French legislation satisfied all the requirements of the Convention**.

41. This ground for inadmissibility is provided for in Article 35(1) of the Convention, which states that: "*The Court may only be seized after all domestic remedies have been exhausted, as provided by the principles of general international law, and within a period of six months from the date of the final domestic decision.*"

42. The possibility of referring a complaint to the commission for this purpose is provided for in Articles L. 833-4 and L. 854 9 of the French Internal Security Code. See also section 2 of this report, p. 91 et seq.

43. This subsidiarity is enshrined in the preamble to the Convention.

44. See Articles L 833-4 and L. 841-1 of the French Internal Security Code.

45. See in particular the judgments of the Grand Chamber, ECHR, 25 May 2021, Big Brother Watch and others v. the United Kingdom, No. 58170/13, and Centrum för rättvisa v. Sweden, No. 35052/08.

The court first noted that any person may ask the CNCTR to ensure that they are not being illegally monitored using intelligence-gathering techniques. It also relies on the commission's independence from the executive branch, based on the provisions of the French Internal Security Code relating to its composition, the appointment of its members and its chairman, and the non-renewable nature of their terms of office[46]. It is also recalled that the members and agents assisting them are bound by national defence secrecy[47], have permanent, full and direct access to the data obtained from surveillance and may request from the Prime Minister any other information necessary for the performance of their duties[48]. In addition, although the commission cannot itself order the interruption of a surveillance measure and the destruction of the information collected, but can only make recommendations to that effect, its chairman or at least three of its members may lodge an appeal before the Council of State if such a recommendation is not followed.

The court then considers the appeal that persons who are not satisfied with the CNCTR's response may lodge with the Council of State[49]. This appeal is brought before a specialised panel of that court, whose members, as well as the public rapporteur, are authorised to hear matters covered by national defence secrecy. The member of the panel responsible for investigating the case carries out the necessary checks without communicating the information obtained to the applicant or their counsel. On the day of the hearing, if the panel hears their oral observations, it invites them to withdraw before the public rapporteur delivers their conclusions.

The applicants criticised the infringement of the principle of adversarial proceedings, which prohibits a judge from basing

46. See Articles L. 831-1 et seq. of the French Internal Security Code.

47. See Article L. 832-5 of the French Internal Security Code.

48. See in particular Article L. 833-2 of the French Internal Security Code.

49. This appeal, provided for in Article L. 841-1 of the French Internal Security Code, is exercised under the conditions set out in Articles L. 773-1 et seq. and R. 773-7 et seq. of the French Code of Administrative Justice.

a decision on elements that the parties have not been able to examine, as well as a violation of the principle of equality of arms. While the court does note that the procedure departs from ordinary law by adapting the adversarial process to reconcile the requirements of a fair trial with the need to preserve national defence secrecy, **it considers that this restriction is offset by robust procedural safeguards**. The judges are authorised to access classified information and may examine all the evidence necessary to perform their duties, which they obtain through extensive investigative powers. In addition, the CNCTR is informed of the filing of the application, may submit observations and is then provided with all the documents produced by the parties. Finally, the specialised panel is not limited by the grounds invoked by the applicant but may raise any ground of its own motion, contrary to the normal rule in administrative justice.

Thanks to this procedural mechanism, the Council of State rules with full knowledge of the facts and may address illegalities that the applicant has not necessarily raised because they were not brought to their attention. Where it finds an irregularity, the specialised panel is able to take appropriate corrective action by, if necessary, revoking the authorisation to use an intelligence-gathering technique and ordering the destruction of information gathered. If the applicant so requests, it may order the State to compensate for the damage suffered; if it finds that an offence has been committed, it must notify the public prosecutor.

Another criticism raised by the applicants concerned the reasoning behind the decisions handed down at the end of the procedure. Indeed, similar to the responses provided by the CNCTR to individuals who contact it, these decisions inform the applicant either that no illegality has been identified, which does not exclude the possibility that they have been subjected to one or more intelligence-gathering techniques in compliance with the law, but

may also mean that they have not been subjected to any such techniques, or that an illegality was identified but has since been remedied, without specifying the nature of the illegality, as such information would risk compromising national defence secrecy.

The court accepts that this minimal reasoning is justified by the requirements of protecting national defence secrecy, recalling that the European Convention does not require remedies to be structured in a way that would reveal to complainants whether surveillance has been conducted, and does not preclude a "neither confirm nor deny" approach.

Having thus recognised the effectiveness of the remedies provided for by French law, the Court examined whether there were special circumstances that could lead to the obligation to exhaust domestic remedies being set aside in this case. The applicants could have dispensed with submitting to the Council of State arguments based on the incompatibility of French legislation with the European Convention if they had encountered well-established case law to the contrary. However, although the Constitutional Council had ruled in 2015 on the constitutionality of French legislation on intelligence[50], the Council of State had not, at the date the applications were brought before the court, taken a position on its compatibility with the Convention. It had the opportunity to do so subsequently, in decisions which the court analysed in its judgment[51].

50. See Decision No. 2015-713 DC of 23 July 2015 on the Intelligence Act.

51. Thus, the specialised panel ruled that the legal remedy available in the field of intelligence-gathering techniques constitutes an effective remedy within the meaning of Article 13 of the Convention (Council of State, 6 November 2017, No. 408495), that the applicable rules do not place a disproportionate restriction on the adversarial nature of the proceedings or the principle of equality of arms as guaranteed by Article 6§1 (Council of State, 22 March 2024, No. 476054, point 9), that the provisions governing the implementation of intelligence-gathering techniques do not infringe the right to respect for private life guaranteed by Article 8 (same decision, point 8), and that the specific provisions concerning lawyers, which prohibit them from being placed under surveillance in connection with their professional activities, do not infringe either the right to respect for private life or the rights of the defence (Council of State, 22 March 2024, No. 474404). These decisions take a position on the compatibility of French legislation with the Convention. Moreover, the specialised panel ensures in each case that any measures implemented comply with the requirements of Article 8, without being required to provide reasoning on this point where there has been no violation of that article (Council of State, 6 November 2017, No. 408495, point 7, and Council of State, 22 March 2024, No. 476054, point 11).

Thus, although the court dismissed the applications before it as inadmissible, it was only able to do so by ruling on **the effectiveness of remedies in relation to intelligence-gathering techniques** and on the **fairness of the rules of procedure**, establishing the decisive role of the intervention of the CNCTR and then of the specialised panel of the Council of State in this matter and, in fact, taking a significant position on the substance of the dispute.

However, its decision does not rule on the other complaints raised by the applicants relating in particular to the protection of journalists' sources, freedom of expression, control of international surveillance measures and the collection and use of information from foreign services. These issues are nevertheless clarified by the court's case law resulting from previous judgments.

For the most part, they are dealt with by French legislation in a manner that appears to satisfy the requirements of the European Convention. However, as the commission has already had occasion to point out on several occasions, the same cannot be said of the treatment by the French services of information provided by foreign services or, symmetrically, information transmitted to these services by the French services[52].

52. On this point, see in particular the CNCTR's 8th activity report for 2023, p. 82 et seq., and the 6th activity report for 2021, p. 48 et seq. See also the proceedings of the symposium held on 15 October 2024, issue 4 of the journal *Etudes françaises de renseignement et de cyber* (EFRC), p. 122.

3.2. Specific amendments to the legislative framework on intelligence whose scope cannot be assessed at this stage

In its previous activity report, the CNCTR emphasised that the legislative deadline in 2025 for reviewing the future of satellite security interceptions, introduced on an experimental basis in 2021 in the French Internal Security Code (see box on p. 48 of this report), was an opportunity to develop the legal framework towards greater compliance with European requirements and greater consistency and effectiveness[53]. In view of the decision of the European Court of Human Rights analysed above, which found no violation of the Convention – without, however, ruling on all aspects of the French legal framework – the government has decided not to introduce a bill to this effect for the time being. In this context, it is therefore parliamentary initiatives, each with a more limited scope, which have recently amended or are preparing to amend this legal framework in a very targeted manner.

3.2.1. The law of 25 July 2024 aimed at preventing foreign interference in France extended, on an experimental basis, the so-called algorithm technique[54] to new purposes

Directly inspired by the work of the Parliamentary Intelligence Committee on this subject[55] and based on a proposed law[56], law no. 2024-850 of 25 July 2024 aimed at preventing foreign

53. See the CNCTR's 8th activity report for 2023, p. 81 et seq.

54. See the section on this technique on p. 135 et seq. of this report.

55. See the public report on the activities of the Parliamentary Intelligence Committee (DPR) for the year 2022-2023: https://www.assemblee-nationale.fr/dyn/16/rapports/dpr/l16b1454_rapport-information#

56. Bill No. 2150 proposed by Mr Sacha Houilé, Ms. Constance Le Grip and Mr Thomas Gassiloud, submitted to the National Assembly on 6 February 2024.

interference in France has, through its Article 6, temporarily extended the provisions of Article L. 851-3 of the French Internal Security Code concerning the so-called algorithm technique[57] to the purposes referred to in points 1 and 2 of Article L. 811-3 of the same code. The automated processing operations provided for under these provisions, previously limited to the objective of preventing terrorism, may now be implemented to detect connections likely to reveal foreign interference or threats to national defence. Although integrated into the French Internal Security Code, these amending provisions are only applicable until 31 July 2028[58] and must be the subject of a report to Parliament no later than two years before that date, meaning that they retain an experimental character.

As at 31 December 2024, this new possibility had not been used by the specialised intelligence services (see p. 42 of this report). The commission is therefore unable to assess its practical impact in terms of both the intensity and effectiveness of surveillance.

3.2.2. The bill aimed at freeing France from the trap of drug trafficking seeks to strengthen the use of administrative intelligence in the fight against organised crime

On 28 and 29 April 2025, following the report produced on behalf of the Senate's commission of inquiry into the impact of drug trafficking in France and the measures to be taken to address it[59], the bill "*aimed at freeing France from the trap of drug trafficking*" was

57. See the analysis of the algorithm technique on p. 135 of the report.

58. The provisions of Article 8 of the draft law on drug trafficking postpone this deadline to 31 December 2028. This text was the subject of three referrals to the Constitutional Council on 12 May 2025. As of the date of finalisation of this report, the decision of the Constitutional Council is not yet known.

59. Senate, report no. 588 of 7 May 2024, by Mr Jérôme Durain and Mr Etienne Blanc, *A necessary wake-up call: escaping the trap of drug trafficking.*

adopted by Parliament[60]. However, Title III of this text contains provisions intended to strengthen the work of the intelligence services in the fight against drug trafficking.

Thus, building on the experimental framework introduced by the law aimed at preventing foreign interference mentioned in the previous section, Article 8 of the draft law establishes a trial period intended to extend the use of the so-called algorithm technique, provided for under Article L. 851-3 of the French Internal Security Code, to part of the purpose referred to in point 6 of Article L. 811-3 of the same code, namely, the prevention of organised crime and delinquency. The aim is to be able to use this technique to detect threats "*relating to organised crime and delinquency involving offences punishable by ten years' imprisonment insofar as they concern drug trafficking, trafficking in arms and explosive products, smuggling, the import and export of these prohibited goods committed by organised gangs, as well as the laundering of the proceeds thereof*".

Furthermore, Article 8 bis extends the trial of satellite security interceptions from 31 July 2025 to 31 December 2028 (see box on this technique on p. 49 of this report).

Finally, in line with a suggestion made by the commission in its previous report[61], Article 8 ter A aims to align the duration of authorisation to enter a private premises with the duration of the authorisation for the intelligence-gathering technique it supports.

Regardless of the potential implications of these targeted amendments to the legal framework, the commission notes that a more comprehensive reflection on the evolution of the legal framework, a reflection suggested in its previous report, has not yet been initiated.

60. Based on the numbering in the text adopted on 28 and 29 April by the Senate and the National Assembly. This text was the subject of three referrals to the Constitutional Council on 12 May 2025. As of the date of finalisation of this report, the decision of the Constitutional Council is not yet known.

61. See the CNCTR's 8th activity report for 2023, p. 89.

3.3. Advancing the improvement of ex-post control of data collection operations

Beyond certain legislative developments considered, depending on the case, either essential or desirable[62] by the commission in its 2023[63] activity report, the commission had placed particular emphasis on **the need to improve** ex-post **oversight of data collection operations (RDI),** both given the intrusive nature of this technique and the very diverse practices among the services regarding methods of collection and exploitation.

However, it must be noted that while 2024 did indeed see a further increase in the use of this technique[64], the progress made has not achieved all the objectives set by the commission. It therefore intends to continue firmly along this line of effort in 2025.

With regard to relations with the services, notable progress had been achieved in 2023. For one "first circle" service in particular, the commission succeeded in obtaining the establishment of more detailed traceability sheets for data collection operations (RDI). This improvement is a key element in exercising ex-post control, as it clearly defines the framework for collection and allows the identification of elements necessary to prepare these inspections, or even to detect irregularities in advance. The approach is to be welcomed, as it has, for example, made it possible to identify collection methods for which the CNCTR's access was still in its early stages, thus laying the groundwork for greater standardisation.

62. See the CNCTR's 8th activity report for 2023, p. 81 et seq.
63. See the CNCTR's 8th activity report for 2023, p. 78 et seq.
64. See Part 1 of this report on developments in the use of this technique (p. 41).

However, the commission regrets that the expected statistical data could not be provided on a regular basis during 2024. Although their occasional availability confirmed the ability of the service concerned to supervise the implementation of specific procedures, it did not fully contribute to the development of the commission's ex-post control processes, leaving the situation still partly unfinished.

The development of centralised operational tools was undoubtedly the subject that generated the most discussion with the intelligence community in 2024.

As reported by the commission last year, the President of the Republic requested the implementation of a solution to facilitate ex-post control of RDIs by the commission. Postponed until after the Olympic and Paralympic Games, the project was launched in October 2024 under the aegis of the National Coordination of Intelligence and the Fight against Terrorism.

In view of the progress made on this project and the requirements relating to national defence secrecy, the commission is able to report on the following points.

Firstly, it welcomes the fact that it has been closely involved in the design and implementation of the project and naturally calls for its continuation. It is confident that this situation is the result of the strengthening of its technical expertise, driven by Chairman Lasvignes. It is now recognised as a legitimate partner in discussions, regardless of their technical nature. The work carried out since October 2024 has clarified the scope of the project, beyond the initial guidelines and declarations of intent. While the project is now well underway, the commission will remain vigilant in ensuring that the planned timetable, which includes effective implementation in 2027, is adhered to.

With regard to the objective and substance of the project, although the procedures for remote control by the CNCTR have evolved since the initial drafts at the end of 2023, its effectiveness is a prerequisite and the architectural proposals formulated at this stage meet this criterion.

Complexity issues have been clearly identified and the commission will be vigilant to ensure that the project continues under satisfactory conditions. It is firmly committed to the success of this initiative alongside the other project partners. This is a major lever for strengthening its ex-post control of RDI. The year 2025 must therefore firmly build on this initial trajectory, with the goal of having an operational system in place by 2027.

Finally, **the commission reiterates the importance it attaches to the implementation, by a major service, of the measures it undertook to take to facilitate access to intelligence reports drawn from the exploitation of RDI pending the establishment of a more comprehensive system**.

10 YEARS OF THE CNCTR

"The CNCTR is at the heart of democracy. […] The CNCTR is an essential body for the vitality of our democracy, the preservation of our freedoms, and the reconciliation of security, the effectiveness of services and the preservation of individual rights and freedoms."

Mr Loic Kervran, Member of Parliament for Cher[65]

"The CNCTR therefore plays a considerable role in regulating intelligence services."

Mr Guillaume Larrivé, former Member of Parliament for Yonne[66]

3 October 2025[67] will mark the 10th anniversary of the National Oversight Commission for Intelligence-Gathering Techniques.

Over the past decade, the CNCTR has established itself as a key player within the French intelligence landscape, ensuring rigorous and as transparent as possible oversight, in accordance with the requirements of national defence secrecy, of the activities of the intelligence services governed by the French Internal Security Code. In line with the principles set out by law, this oversight aims to strike a balance between the protection of individual freedoms and the safeguarding of the Nation's fundamental interests.

To mark this anniversary, the commission will organise a symposium on 22 September 2025.

65. Hearing of Serge Lasvignes before the National Assembly, 22 September 2021.
66. Idem.
67. Effective date of appointments of the various members of the first college of the commission.

The tools of surveillance

File 1. Equipment used to infringe on privacy

File 2. Algorithms

File 1. Equipment used to infringe on privacy

Study: The discreet appeal of Articles R. 226-1 et seq. of the French Criminal Code: Regulation of the sale and possession of equipment that can be used to commit violations of privacy and the issues involved

In 2015, as part of the Intelligence Act of 24 July 2015, the French legislature chose to design and organise the control of intelligence services[1] activities through the prism of intelligence-gathering techniques strictly limited by the French Internal Security Code.

However, the existence of legal authorisation to implement a technique, whether it be the interception of a telephone communication or the collection of data stored in a computer system, would be ineffective if it were not accompanied by the possibility for the service to technically carry out these operations. In other words, without the means to conduct surveillance, the authorisation to conduct surveillance is meaningless. However, the intelligence services' practical ability to implement authorised techniques increasingly depends on maintaining a level of technical capability proportionate to the current pace of technological developments in electronic communications, and more broadly, in digital tools.

1. Law no. 2015-912 of 24 July 2015.

The actual scope of an authorisation to implement an intelligence-gathering technique cannot therefore be fully assessed without also considering the functions and status of the surveillance and interception tools it mobilises. Beyond strictly legal issues, this concerns the structure and dynamics of a particular market, that of surveillance technologies.

The advisory commission established by Article R. 226-2 of the French Criminal Code[2], whose secretariat is provided by the French Cybersecurity Agency (ANSSI), plays a central role by issuing the authorisations required, in particular, for the manufacture, sale, or acquisition of equipment used to carry out the technical surveillance measures provided for under Book VIII of the French Internal Security Code. In doing so, it operates at the intersection of two essential dimensions.

On the one hand, its existence reflects the intention to provide a continuous and coherent set of legal safeguards for the protection of privacy. In a technology market where grey areas are increasingly common, acquiring technical capabilities subject to regulatory control is, at times, surprisingly easy, including on mainstream e-commerce platforms. The so-called "R. 226 commission" remains the only body structuring this sector in France.

Furthermore, by issuing different authorisations depending on whether the end user of such devices is authorised to produce intelligence within the meaning of the French Internal Security Code or can justify other grounds for such use, the "R. 226" commission contributes to the control of public authorities and the regulation of the private market. In this dual capacity, it is the material basis of surveillance that is subject to scrutiny and questioned in accordance with the aims of the rule of law.

2. All of the provisions of the French Criminal Code mentioned in the study are included in Appendix 5 of this report.

This study therefore aims to demonstrate both the necessity and relevance of the current legal framework and how the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR) contributes, together with all the partners involved, to the control of constantly evolving technologies.

1. The oversight exercised by the "R. 226" commission is in line with the missions assigned to the CNCTR concerning the protection of privacy and the regulation of surveillance techniques

1.1. The establishment of a strict regulatory authorisation framework for surveillance technologies is a prerequisite for the protection of privacy

1.1.1. The various uses of technical devices that enable the interception of private communications, data, or conversations constitute criminal offences in the absence of a legal basis assessed by the "R. 226" advisory commission

The French Criminal Code defines several offences relating to invasion of privacy. In particular, it is prohibited to capture, record or transmit, without the consent of the person concerned, words spoken in private or in confidence, or to fix, record or transmit the image of a person in a private place. Entering a private home, collecting personal computer data or geolocating a person without their knowledge, as well as storing and sharing information gathered by these various means, also constitute offences. By extension, on the one hand, the manufacture, importing, exhibiting, offering, renting and selling, and on the other hand the acquisition and possession of devices likely to enable or

facilitate the commission of these various infringements of privacy, whether directional microphones, miniature cameras or devices for intercepting telephone communications, are also punishable by law.

Article 226-3 of the French Criminal Code specifically punishes three "technical intrusions" of privacy:

- access to electronic communications (see Article 226-15 of the French Criminal Code),
- the recording of words spoken in private (see Article 226-1 of the French Criminal Code),
- and the collection of computer data (by reference to Articles 706-102-1 of the French Code of Criminal Procedure and L. 853-2 of the French Internal Security Code).

This article further provides that the offence may be committed even where the constituent acts are committed through negligence, "in the absence of ministerial authorisation".

It also regulates the advertising that may be carried out, which must not amount to an incitement to commit the aforementioned offences.

Both administrative and judicial surveillance measures necessarily infringe upon privacy and are therefore, by definition, exceptions to ordinary law, which provides multiple safeguards to protect personal privacy and private life.

It is worth noting in this regard that Book VIII of the French Internal Security Code opens with the sovereign exception that permits infringements of the right to privacy "*only in cases of public necessity provided for by law, within the limits set by law, and in compliance with the principle of proportionality*" (see Article L. 801-1 of the French Internal Security Code). This principle underpins the existence of a "*public intelligence policy*" carried out by the services in pursuit of purposes strictly defined by law, for which such infringements are considered legitimate (see Articles L. 811-1 to L. 811-3 of the same code).

The same concern for consistency, which leads the French Criminal Code to link the punishment of privacy violations to the trade in the means enabling them to be carried out, also implies that the intelligence services must have legal authorisation to possess the devices enabling them to carry out their missions.

An authorisation regime has therefore been established within the French Criminal Code to control, on the one hand, the marketing of such devices (Article R. 226-3 of the French Criminal Code) and, on the other hand, their acquisition by private or public entities (Article R. 226-7 of the French Criminal Code). This comprehensive interpretation of the dangers, as well as the need for surveillance, its intentions and its means, is a unique feature of French law, which the "R. 226" advisory commission is responsible for implementing.

1.1.2. The "R. 226" advisory commission monitors these devices throughout their life cycle and use

Article R. 226-2 of the French Criminal Code establishes the advisory commission responsible for assisting the Director of the French Cybersecurity Agency (ANSSI), who ultimately holds the responsibility for issuing authorisations for the sale and acquisition of devices, the nature of which is defined by ministerial order[3]. Its composition, set by the same article at eleven members, reflects its strong inter-ministerial dimension, with representatives from the Ministries of Justice, the Interior, the Armed Forces and the Economy, and its openness to administrative authorities (the CNCTR and the National Frequency Agency, ANFr, are thus represented) and technical expertise (two qualified experts are appointed by the Prime Minister).

3. This list indicates the different categories of equipment subject to "R. 226" authorisations. The commission must first assess, in each case, whether a specific device submitted by an industrial company requesting, for example, authorisation to sell on the national territory, is actually covered by this list. The latest decree in force is the decree of 4 July 2012 establishing the list of technical equipment and devices provided for in Article 226-3 of the French Criminal Code.

This commission evaluates each surveillance device, whether hardware or software, in all aspects of its life cycle and according to the nature of the request submitted. Whether it concerns importing a data collection device into national territory, demonstrating such a device at a specialised trade fair, or using it within an intelligence service, authorisation must be issued by the director general of ANSSI, based on the opinion of the "R. 226" advisory commission. The procedure provided for in Article R. 226-4 of the French Criminal Code requires that the device in question be subject to a technical presentation or even a full expert assessment in order to determine its uses, risks and target market. The authorisation issued is then adjusted in terms of its duration, which may be up to six years, and its scope, with restrictions on use where necessary, and the introduction of traceability of the device based on its authorisation number (Article R. 226-6).

The high technical nature of the devices submitted for collective assessment, as well as the significant issues at stake in terms of privacy protection, require rigorous monitoring of requests, which is carried out by the ANSSI secretariat. The possibility for the commission to reserve its opinion or make it conditional on presentations by the companies requesting it also makes it possible to issue authorisations on the basis of the most complete information possible. With an average of one meeting every two months, approximately 1,500 authorisations are issued each year, within the meaning of Articles R. 226-3 and R. 226-7 of the French Criminal Code[4]. These opinions are gradually shaping a doctrine at the heart of public regulation of surveillance and interception technologies.

4. See interview with Mr Vincent Strubel, p. 129 et seq. of this report. The ANSSI activity reports show that 1,567 decisions were made in 2023, including 22 refusals, and 1,610 decisions were made in 2024, including 52 refusals.

1.2. The provisions of articles R. 226-1 et seq. of the French Criminal Code provide the CNCTR with an additional means of controlling the activities of the intelligence services

1.2.1. While intelligence services are by definition authorised to use the devices referred to in Articles R. 226-1 et seq. of the French Criminal Code and benefit from a specific authorisation regime, their use and inventories are subject to controls by the CNCTR

The "R. 226" commission, as we have seen, has a broader mission than simply supervising the intelligence services. It is, in fact, the first port of call for anyone wishing to enter the surveillance market in France in any capacity. It goes without saying, however, that the intelligence services, without being able to derogate from the obligation to obtain the appropriate authorisations for the equipment they use, occupy a special place in this economy.

State services may benefit from a simplified formal procedure. Taking into account, where applicable, the service's legal entitlement to use such equipment, the requirement to submit individual authorisation requests for each device held is replaced by the maintenance of a register within each service, accessible to the CNCTR, which records all equipment in the entity's possession. This authorisation, known as "*de plein droit*" (APD), meaning automatic or by operation of law, is provided for under Article R. 226-9 of the French Criminal Code), is re-evaluated at regular intervals[5] during formal sessions, the composition of which is

5. In practice, this is done every three years, at the same time as for all acquisition/possession requests.

restricted to ANSSI and the CNCTR due to the sensitive nature of the information exchanged. During these sessions, particular attention is paid to the organisation of the service regarding the management and oversight of the equipment, the quality of the register, any changes to the legal basis for the use of these capabilities, and the absence of anomalies during the period under review.

Similarly, the Defence Code provides for and regulates the use of devices on national territory, for testing purposes only, by certain units under the authority of the Ministry of the Armed Forces. The CNCTR is also responsible for monitoring these operations; Article L. 2371-2 of the Defence Code stipulates that such activities must be declared in advance to the CNCTR[6]. The latter is thus able to verify both the conditions of acquisition and possession of intelligence-gathering equipment and the procedures for its use, on a case-by-case basis, whether under authorisations issued by the Prime Minister under Book VIII of the French Internal Security Code or for testing purposes.

6. Article L. 2371-2 of the Defence Code: "Subject to prior notification to the National Commission for the Oversight of Intelligence-Gathering Techniques, the Ministry of Defence service responsible for certifying the equipment or technical devices referred to in point 1 of Article 226-3 of the French Criminal Code for the benefit of the armed forces and Ministry of Defence services, on the one hand, and members of military units of the armed forces designated by ministerial order of the Minister of Defence, on the other hand, are authorised to carry out tests of equipment or devices enabling the implementation of the techniques or measures referred to in Article L. 851-6, Article L. 852-1 (II), and Articles L. 852-2, L. 854-1, and L. 855-1 A of the French Internal Security Code. These tests are carried out by individually designated and security-cleared agents, strictly for the purpose of performing these technical operations, excluding any exploitation of the data collected. This data may only be retained for the duration of these tests and must be destroyed no later than upon completion of the tests. The National Oversight Commission for Intelligence-Gathering Techniques shall be informed of the scope and nature of the tests carried out under this article. To this end, a register listing the technical operations performed shall be provided to the commission upon request. The conditions for the application of this article shall be determined by order of the Minister of Defence, issued after consulting the National Oversight Commission for Intelligence-Gathering Techniques."

1.2.2. The activities of the "R. 226" advisory committee are an opportunity for the CNCTR to address the major challenges of the legal framework from a specific technical, economic and legal perspective

The CNCTR ensures that the intelligence-gathering techniques strictly provided for in the French Internal Security Code are implemented in accordance with their legal framework. The cross-cutting nature of surveillance, especially in today's digital environment, nevertheless requires that independent oversight draw on multiple approaches and not rely solely on legal formalities.

The CNCTR contributes to the deliberations of the "R. 226" advisory commission by providing its legal expertise on privacy violations or administrative policing issues specific to the activities of the intelligence services. In return, it benefits from the presentations and debates to update its own understanding of the technological issues underlying the use of the techniques listed in Chapter V of Book VIII of the French Internal Security Code. The diversity of both the equipment examined and the associated scenarios of use[7] enables the commission to broaden its knowledge of surveillance tools and thus to monitor new technical developments effectively, which usefully complements the exchanges it has established with the intelligence services.

The "R. 226" commission, beyond its administrative name, therefore constitutes an original forum for continuing dialogue with the intelligence services on a variety of topics, closely reflecting their operational and budgetary concerns. It also makes it possible to highlight difficulties specific to developments in the information economy when these come up against issues of sovereignty, such as the growth of the European internal market for telecommunications operators.

7. The same product can be used for completely different purposes and within completely different regulatory frameworks.

2. The development and dissemination of technological resources covered by the so-called "R. 226" regulations has not accelerated a legal framework that remains appropriate and effective for supervisory authorities

2.1. The strict authorisation regime provided for in the French Criminal Code leads to close dialogue between the "R. 226" commission and those involved in the production, sale and use of the equipment and devices concerned

2.1.1. Authorisation is granted following a sometimes extensive dialogue with manufacturers, distributors and users of the devices concerned

The "R. 226" advisory commission meets mainly to examine the authorisation requests submitted to it. It issues several hundred opinions during the six meetings generally scheduled each year. During these meetings, it also collectively monitors the progress of longer-term cases that may affect its assessment of certain categories of equipment. The commission examines issues relating to potential infringements of privacy posed by products available on the market and, where necessary, takes classification decisions. From that point onwards, each stage (manufacture, import, display, offer, rental, sale, acquisition, possession) is subject to authorisation.

For example, in 2022, the advisory commission proposed the classification of digital investigation equipment on mobile phones, which is used in particular by investigative services and expert appraisers, in view of the use that everyone now makes of their mobile phones and the ever-increasing functionality of these devices.

In addition to this regular activity, the commission liaises directly with certain applicants to clarify their requests. In the case of manufacturers or suppliers, it is sometimes necessary to obtain detailed technical information, for example on the list of data collected or the expected performance according to the scenarios of use. In the case of acquisition requests, the commission is vigilant about the legal basis invoked to justify the possession of the devices. It is therefore common practice to request additional information from entities, whether private or public, so that they can describe the context of use, the applicable texts, and the storage conditions and logistical monitoring of the equipment to prevent any misuse.

2.1.2. The "R. 226" commission bases its opinions on usage profiles that assess the intrusiveness of the device analysed in each case

In its analysis of equipment, the "R. 226" commission first assesses whether they can be used to commit the offences provided for in the French Criminal Code mentioned above and, if so, whether their very purpose is to enable the commission of such offences. Depending on the results of this assessment, the equipment will be classified, or not, as falling under the "R. 226" regulations and subject to authorisation, regardless of its potential user and the legitimacy of its activity. However, depending on the intrusive nature of the equipment in question, some equipment is made available only to certain users in accordance with the functions assigned to them by law.

Next, an applicant, who may represent a legal entity, may apply to the director general of the ANSSI for one of the authorisations listed above. The commission then assesses the legal basis of the request, as well as the risks that would be incurred by granting the authorisation. Ultimately, ANSSI grants, postpones or refuses authorisation based on the opinions of the advisory commission, which are based in particular on the principles of necessity and proportionality.

The assessment of necessity is based primarily on an analysis of the legal bases that the applicant can invoke. Thus, for a government service, it is normal for a legislative or regulatory provision to justify the use of technical devices covered by the "R. 226" authorisation regime. The type of device may sometimes be explicitly mentioned or follow logically from the suitability of a regulated process and its intended technical use. If this is not the case, the commission assesses the admissibility of the request, taking into account the practices of the business sector concerned and the issues at stake; this approach is often based on wider consultations.

The commission, seeking to ensure that action is both consistent and robust, has defined usage profiles. These are designed to protect individual freedoms without unduly hindering the economic operators concerned. The profiles are based on the diversity of equipment available on the market. Thus, for the same technical purpose, several categories of products may sometimes be distinguished. Taking the example of digital investigation, a device that only makes a copy of the data would not have the same potential for intrusion as a device that allows both the circumvention of privacy protections (such as an unlock code or password) and the copying of data. In the first case, access to the data would be subject to the prior disclosure of personal secrets, which could mean the prior information and consent of the owner. The commission therefore assesses the proportionality between the justified use and the intrusive nature of the equipment requested.

In this regard, there is a certain continuity between the questions of proportionality submitted to the CNCTR on a daily basis in the processing of requests for intelligence-gathering techniques by the services, on the one hand, and the assessment of the degree of invasion of privacy of a particular device before the "R. 226" commission, on the other.

2.2. The administrative and judicial control of devices covered by Articles R. 226-1 et seq. of the French Criminal Code, far from hindering innovation, contributes to the structuring and efficiency of this market

2.2.1. The infrastructure and devices required for technical surveillance are constantly evolving and becoming more complex, without however rendering the legal framework obsolete

As with algorithms, it is tempting to view the development of the surveillance market as the expression of a vague, highly technical and very dynamic threat against which the law is powerless. The dynamism of the industrial sector is undeniable. It is developing in several directions and on multiple scales: interception mechanisms for telecommunications operators to comply with legal requirements[8]; hardware or software, "*specifically designed to access, record, store and transmit computer data without the consent of the persons concerned*"[9] and "*remote sound interception devices such as microphones or devices equipped with*

8. See the order of 11 August 2016 amending the order of 4 July 2012 cited in note 3 above.
9. See point 3 of Appendix I to the order of 4 July 2012 cited in note 3 above.

acoustic amplification devices"[10]. The range of devices covered by the "R. 226" regulations is therefore broad and constantly evolving.

However, regardless of the current technological proliferation, the procedure outlined above represents a structuring step for both private and public stakeholders operating in this market, by providing them with legal certainty. In this sense, the legitimate concerns that may arise from the relative "democratisation" of access to such devices should be placed into perspective.

On the one hand, the technical characterisation of the relevant devices is set out in the aforementioned decree and can therefore be easily updated by the Prime Minister without requiring the French Criminal Code to be revised each time a new technology is introduced. On the other hand, the fact that the authorisations required for the lawful distribution of these devices are dealt with at a single point makes it possible to take a cross-cutting approach to the market. The absence of a legal time limit for the granting or refusal of an authorisation allows the commission to take the time necessary to assess new devices.

2.2.2. The authorisation regime allows this market and these technologies to manage the legal risks clearly set out in the French Criminal Code, while also serving as an important tool for protecting privacy and individual freedoms

The public regulation of surveillance technologies, as contributed to by the "R. 226" advisory commission, is mainly concentrated in the initial authorisation phase. It is at the time of submission of an application for marketing, manufacture or transfer, where applicable, that the public authorities have the opportunity to

10. See point 2 of Appendix I to the order of 4 July 2012 cited in note 3 above.

assess the dangers inherent in a technical device. Ex-post control raises specific difficulties, particularly in view of the considerable judicial resources that would be required for the systematic control of authorisations granted.

However, it should be noted, on the one hand, that this control exists and can have a clear deterrent effect, for example when the illegal display of unauthorised equipment at a trade fair leads to the immediate arrest of the exhibitors and the seizure of the products. The legal risk is therefore clearly expressed and present in the minds of the various players in this particular market. For a company specialising in the design and sale of surveillance devices, maintaining legal authorisation, the withdrawal of which is explicitly provided for by the legislator (see Article R. 226-11 of the French Criminal Code), can represent an existential threat by prohibiting access to the French market.

Furthermore, as mentioned above, devices covered by the "R. 226" regulations contribute to the effectiveness of the intelligence services and are therefore fully subject to the CNCTR's control. The ability to demand accountability, during an on-site inspection, for the use of a device whose traceability and serial number are directly accessible to the CNCTR, represents a significant tool for enhancing the credibility, intensity, and precision of such oversight. More broadly, the various public authorities that may seek to acquire similar devices, beyond the narrow scope of the intelligence services, are aware that they must comply with the advisory procedure of a commission whose pluralistic composition promotes impartiality.

In all these respects, the legal framework within which the "R. 226" commission operates provides relevant tools to regulate the development of technologies, the uncontrolled proliferation of which could pose serious threats to privacy.

Interview with Mr Vincent Strubel, Director General of French Cybersecurity Agency (ANSSI)

Could you briefly outline the missions of ANSSI and more specifically place the R. 226 activity within that framework?

Under the authority of the Prime Minister and attached to the General Secretariat for Defence and National Security (SGDSN), ANSSI is uniquely positioned to deploy a comprehensive cybersecurity policy and ensure its coordination across ministries. This policy focuses on defending the most critical public and private digital infrastructures. It is also aimed at all those involved in France's digital transformation and promotes conditions for dialogue based on trust with its counterparts at European and international level.

ANSSI is also responsible for the control regime known as "R. 226", derived from Article 226-3 of the French Criminal Code. As such, and in connection with the advisory commission ("R. 226 Commission") established by Article R. 226-2 of the same code, it reviews requests for the sale and possession of products likely to infringe upon the secrecy of communications and privacy.

It thus ensures that these products offer a sufficient level of security to prevent any misuse and are made available only to those actors to whom the law confers a legitimate use for such products.

What resources does the agency dedicate to this activity?

The secretariat of the R. 226 Commission, overseen by ANSSI's regulatory control office, is responsible for the administrative processing of submitted applications. Their technical analysis draws, as needed, on a wide range of expertise available within ANSSI, particularly from the communications security office, which specialises in the analysis and protection of telecommunications networks.

Can you briefly describe the types of products most regularly examined by the Advisory Commission?

Until recently, most of the cases reviewed by the R. 226 Commission concerned two main categories:

- Telecommunications products (such as routers, traffic analysis tools, probes, etc.) and interception devices used by State services as integral parts of electronic communications networks;
- Interception devices used by State services and the armed forces, spectrum monitoring equipment, and so-called "technical surveillance countermeasure" devices (such as scanners).

The end of the 2010s saw the development of forensic analysis devices[11] accessible to the general public, some of which were capable of "unlocking" computer terminals without the consent of their legitimate users, in 2019, the commission extended its remit to include the monitoring of these devices, in order to restrict their use to legitimate players under French law, given their highly intrusive capabilities.

11. Refers to lawful digital investigation. Its purpose is to produce digital evidence (its collection, analysis and preservation) in the context of legal proceedings.

How many decisions do you sign each year?

The number of decisions has been increasing steadily since 2019, with around 270 to 350 products examined per session. Over the last five years, 7,749 decisions have been handed down, an average of 1,550 per year.

Do you have any insight into the regulatory approaches developed by our partners? Are they comparable to the control regime established by the French Criminal Code, or is France deploying a completely original framework?

This system is specific to France and has no equivalent among our partners, even our closest ones. However, some of these partners have expressed interest in our regulations, particularly in view of the positive impact they have had on the security of our electronic communications operators' networks.

The legal framework reserves a place for the R. 226 Advisory Commission in the initial regulation of classified devices. Do you consider that extending ex-post controls is desirable or even necessary? What form might take?

In any case, it would be logical for a body carrying out ex-ante controls based on the provisions of the French Criminal Code to also carry out ex-post controls. The inter-ministerial instruction of 5 September 2006 includes control within the remit of the R. 226 commission (Article 2(3)). At present, ex-post controls are carried out by the Ministries of the Interior and the Armed Forces, as well as by the National Directorate of Intelligence and Customs Investigations (the latter under the Customs Code). The CNCTR is responsible for the oversight of the intelligence services.

ANSSI agents, who do not have judicial police powers, are not responsible for carrying out such controls alone. They can, however,

support these various services by providing technical expertise, including during on-site controls. Such joint teams have already been deployed during controls carried out at specialised trade fairs.

The role of regulator is often subject to attempts at pressure or influence from vested interests. What relationship does the R. 226 Commission have with the relevant economic sectors? How is its authority perceived?

As a general rule, the commission's authority is well accepted by both the administration and industrialists and private users. Discussions with telecommunications and "sensitive" product manufacturers are fluid, thanks in particular to the administrative and technical support provided by the ANSSI and the Defence Electronic Communications Commission (CCED).

The relationship is particularly close with electronic communications operators, who are the target of numerous cyberattack attempts and have fully understood that the controls carried out under R. 226 are a source of continuous improvement in their level of security. They have thus incorporated the processing of their R. 226 applications into an anticipatory approach, making it easier for ANSSI to test the equipment they plan to deploy.

The legal framework remains effective despite rapid technological developments in the field. However, do you anticipate more significant changes that could directly impact the national model?

Or changes brought about by 5G technology, such as containerisation and the use of internal telecommunications clouds developed and maintained by electronic communications operators (OCE), are making it increasingly difficult to view a network function as a "device" within the meaning of regulation R. 226 (platforms and business software are interdependent). This point alone would require a change in the regulatory framework.

Other needs identified relate to satellite, private mobile radio (PMR) or cross-border/pan-European networks, as well as the need to manage the entry of certain players into specific functions (RCS/iMessages). We can also add the reorganisation of the market, with the growing role of passive mobile infrastructure operators (TowerCos), who could position themselves under a RAN as a Service model (where the management of antennas and BTS is no longer handled by the operator and is potentially shared at the vRAN level rather than through RAN sharing). Certain sharing arrangements should undoubtedly also be better formalised, particularly with regard to what should be done on the IT[12] and OTT[13].

Finally, it would be advisable to anticipate the desire expressed by the European Commission to standardise the regulatory framework with a view to creating a single market, which could lead to a revision of national ex-ante authorisation regimes (regulation "R. 226" of the French Criminal Code and Article L. 34-11 of the French Postal and Electronic Communications Code). Close attention should be paid to these developments in order to preserve the essential safeguards for national security currently provided by these provisions.

12. IT refers to telecommunications infrastructure, i.e. the infrastructure of communications operators.
13. OTT refers to "over the top", i.e. a communication or media delivery service without the involvement of a traditional network operator providing the Internet connection.

File 2. Algorithms

Insight: The algorithm: from a simple concept to a complex reality

Gérard Biau,
Professor at Sorbonne University, Director of SCAI (Sorbonne Centre for AI) and member of the French Academy of Sciences

Mr Arnaud Latil,
Senior Lecturer at Sorbonne University, member of SCAI and CERDI (University of Saclay)

The word algorithm originates from the name of the 9th-century Persian mathematician Al-Khwârizmî. He authored a major work entitled "The Compendious Book on Calculation by Completion and Balancing", which also gave rise to the term algebra. The word algorithm is a deformation of the medieval Latin *algoritmi*, which referred to the calculation processes inspired by Al-Khwârizmî's work. This term was used by Latin translators to name the methods of calculation and problem solving described in his work, particularly those based on the decimal number system introduced in Europe from the Arab-Islamic world.

In modern language, an algorithm can be defined in several ways depending on the context. In computer science, it is a finite sequence of instructions or logical operations that solve a problem or accomplish a specific task. More generally, an algorithm can be seen as a method or systematic process for achieving a given goal, whether in mathematics, social sciences or other disciplines.

A recipe, for example, is an algorithm in that it describes a structured and ordered process for achieving a specific goal, in this case the preparation of a dish. Other classic examples include Euclid's algorithm, used to calculate the greatest common divisor of two numbers, or sorting algorithms (such as bubble sort or quicksort), which are used to arrange a list of elements in order.

In our daily lives, algorithms are at the heart of many contemporary systems. Search engines such as Google Search use sophisticated algorithms to rank billions of web pages. Streaming and information platforms (Netflix, Facebook, etc.) use recommendation algorithms to personalise the news feed according to each user's preferences. Financial systems use trading algorithms to execute transactions in a fraction of a second.

Since the 2000s, algorithms have undergone a profound transformation driven by artificial intelligence and the development of machine learning. These technologies, which are largely based on complex models (deep neural networks, transformer architectures, etc.) trained using huge volumes of data, mark a break with traditional algorithms. Now, it is no longer just a matter of explicit, programmed rules, but of systems capable of learning, evolving and adapting their responses based on the data they ingest. The development of these systems requires enormous computing power, made possible by exponential advances in IT hardware, particularly through graphics processing units (GPUs). These infrastructures make it possible to train large models (known as foundation models) of unprecedented complexity, capable of processing multimodal data

(text, images, videos, etc.), efficiently performing increasingly spectacular tasks, or detecting patterns invisible to the human eye.

This new landscape blurs the notion of algorithms, repositioning them at the frontier between the models themselves, their training, industrial expertise, and the feedback loops generated by interactions with users. Is ChatGPT, for example, simply an algorithm? Or is it an industrial product, shaped by strategic choices, statistical methods and collected data? It illustrates the grey area where technology, human expertise and collective behaviour combine to produce a tool that is greater than the sum of its parts.

The convergence of data, algorithms and artificial intelligence is opening up a new field at the crossroads of science, engineering and the humanities. This new ecosystem raises fundamental questions about transparency, accountability and the balance of power. Who controls these systems, and in whose interests? Where does the algorithm end and industrial strategy begin? This is no longer just a technical issue: it is a cultural and societal revolution, where the rules of the game are being redefined.

From a public policy perspective, algorithms are subject to emerging frameworks that differ across countries, cultures and continents. In Europe, despite this growing complexity, the regulation of algorithms and automated data processing systems still falls within a legal framework with traditional objectives and methods, mainly based on the objectives of transparency, explainability and control. Personal data law, administrative law, health law and artificial intelligence law thus provide for information obligations, and in some cases explanation obligations, when algorithms are used. The GDPR and the recent AI Regulation are emblematic examples of this. Where algorithmic uses are likely to more seriously undermine rights and freedoms, the legislator then deploys inspection or audit procedures, as is the case, for example, for content moderation and recommendation algorithms used by platforms, as provided for in the Digital Services Act.

In the most serious cases of infringement of freedoms, prior authorisation from the administration is then required, as is the case for certain intelligence-gathering techniques.

However, these legal tools are hampered by the growing complexity of algorithms, combined with their increasing role in the economy, information, employment and education. In response, a new generation of legal tools is taking shape. These tools are part of a so-called "risk-based" approach, which consists not only of adjusting the stringency of legislative action according to the perceived severity of algorithmic uses, but also, and above all, of assessing their consequences for society. In terms of legislative methods, the development of experimental laws and regulatory sandboxes reflects this realistic view of algorithmic complexity. The introduction of scores, such as the "cyber score", or risk mapping obligations for operators, is part of this algorithmic monitoring approach.

However, there remains a category of risks that is even more sensitive and daunting, and understanding them poses a major challenge for public policy: systemic risks. This term refers to the risk of widespread disruption of an entire organised system, such as the financial system, the healthcare system or the democratic system. The major financial crisis of 2008 helped bring systemic risks to the forefront: the uncontrolled circulation of "toxic assets" through securitisation mechanisms, neither regulated nor even properly understood by public authorities, led to the collapse of the entire international financial system. Closer to home, the COVID-19 pandemic in 2020 disrupted economic and social organisation on a global scale, demonstrating the scale and power of systemic risks.

In this context, algorithms are at the root of at least two systemic risks. The first relates to information risks and the circulation of knowledge and expertise. With the development of generative artificial intelligence tools, symbolised by ChatGPT, the loss of control over information is becoming a key issue. It is not so much

the risk of errors (the famous "hallucinations" which, in essence, are merely a reflection of the probabilistic nature of the algorithms at the heart of artificial intelligence) or the proliferation of deep fakes that are at stake here, but rather the loss of control over the functioning of algorithmic tools. AI algorithms, which have become difficult to audit and are now indispensable, occupy a central place in decision-making and the global flow of information. Their extremely rapid evolution is outpacing public policy.

Partially related to the first, the second systemic risk concerns industrial sovereignty issues. The complexity of large artificial intelligence models, combined with the costs of design and use, raises fears for France and Europe of losing control of the entire algorithmic value chain. From the creation of large models to the production of GPUs, not to mention the "brain drain", the risk of Europe falling behind economically and technologically is very real, as highlighted in the report led by Mario Draghi submitted to the European Commission on 9 September 2024. Not to mention that the most sovereign areas, such as security, justice and defence, are now heavily dependent on algorithms.

Thus, algorithms have evolved from simple objects into complex realities, both technically and politically. For Europe, regulating them requires a genuine industrial strategy that goes beyond the legitimate and necessary objectives of trust, fairness and transparency. Meeting the challenge of this complexity requires an ambitious change of scale and unprecedented responsiveness from public policy. Europe can no longer be content to follow, but must assert itself in the face of new challenges, starting with the quantum revolution that is looming.

Study: Algorithms within the meaning of the French Internal Security Code: from fantasy to legal reality

"Algorithms are the invisible architects of our digital lives. It is time for them to step out of the shadows."[1] It was in these terms that Margrethe Vestager, Vice-President of the European Commission and Commissioner for Competition until November 2024, expressed her support for the actions launched by the Commission at the end of 2023 to demand greater transparency from major online search engines and digital platforms (Apple, Google, Meta, TikTok, Snapchat, YouTube, Amazon, and the social network X) regarding how their content recommendation algorithms operate.

This statement highlights not only the power acquired by the tech giants but also the structuring role played by algorithms, and, by extension, by those who control them, in shaping and driving our digital world.

Usually defined by mathematicians as a sequence of precise instructions that produce a result from input data, the concept of an algorithm[2] is embodied in the digital sphere by a wide variety of automated processes, ranging from the most rudimentary, based on a mathematical formula that is easily understood by everyone, to the most complex, whose sophistication and secrecy give them the appearance of "black boxes".

Like artificial intelligence systems, with which they are often confused, algorithms are omnipresent in public debate[3]. Controlling them has become an essential democratic concern, to the point where these tools are at the heart of regulations being put in place to govern the digital world, particularly at European level.

1. Cited in "The European Parliament asks X for its recommendation algorithms", S. Soarez, Innovations.fr, 17 January 2025. See also the European Commission's publications on the formal proceedings initiated against X on 18 December 2023 and the additional investigation measures sent on 17 January 2025: https://digital-strategy.ec.europa.eu/fr/news/commission-opens-formal-proceedings-against-x-under-digital-services-act and https://digital-strategy.ec.europa.eu/fr/news/commission-addresses-additional-investigatory-measures-x-ongoing-proceedings-under-digital-services.
2. For an introduction to the concept of algorithms, see the contribution by Gérard Biau and Arnaud Latil, "Algorithms: from a simple concept to a complex reality", p. 135 of this report.
3. See also the section on artificial intelligence and intelligence in the 8th activity report for 2023 of the CNCTR, p. 135 et seq.

The intelligence world, which is also marked by the prevalence of digital technologies, is not immune to questions about the use of algorithms to support surveillance.

However, intelligence law is unique in that it has established this mathematical tool as an intelligence-gathering technique in its own right, in addition to providing for its use in processing data collected through surveillance. For example, one of the intelligence-gathering techniques authorised for use by French intelligence services under the French Internal Security Code is automated processing, commonly referred to as an "algorithm", which aims to detect threats or indications of threats by exploiting a large amount of digital data.

ALGORITHMS IN EUROPEAN DIGITAL REGULATION: AN ILLUSTRATION OF THE ISSUES

The European Union's (EU) digital policy has various components aimed at ensuring European competitiveness in this area, regulating its internal market and preserving respect for the rights and freedoms guaranteed in particular by the Charter of Fundamental Rights. Given their importance in the digital space, several of the governance rules laid down by European regulations specifically target algorithms.

The algorithm technique, which is the subject of this study, is not governed by these regulations, as intelligence does not fall within the scope of EU law. However, a brief overview of the texts adopted at European level provides valuable insight into the challenges raised by the control of algorithm use.

Legislation on artificial intelligence: the Artificial Intelligence Act (AI Act)[4]

This text aims to promote the adoption in Europe of human-centric and trustworthy artificial intelligence (AI). It regulates artificial intelligence systems (AIS) placed on the European market to ensure they are safe and comply with existing legislation on fundamental rights, by setting rules

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Digital Services Act).

that all AI developers and deployers must follow, with requirements varying according to the level of risk posed by each system[5].

Algorithms are at the heart of this regulation, as they underpin the development of all complex AIS.

Legislation to regulate the internet: the Digital Markets Act[6] and the Digital Services Act[7]

The Digital Markets Act (DMA) aims to combat anti-competitive practices by internet giants and correct the imbalances in their dominance of the European digital market. It regulates the activities of the largest platforms, particularly those of the major tech giants often referred to by the acronym GAFAM[8], given their role as "gatekeepers", controlling access to the internet. The Digital Services Act (DSA) regulates the activities of digital intermediaries offering their services (internet access providers, cloud services, search engines, content-sharing and trading platforms, social networks, etc.) on the European market, with the main objective of making the web a safer place for users. This regulation provides for measures to combat the spread of illegal and harmful content (incitement to hatred, disinformation, child pornography, etc.) and illegal products and services online (sale of drugs or counterfeit goods, etc.).

To monitor compliance with this legislation, digital companies may be required to shed light on their algorithms, including their content recommendation processes. In its role overseeing and supervising algorithmic systems, the European Commission is supported by the European Centre for Algorithmic Transparency (ECAT), inaugurated on 18 April 2023. The centre's scientists and experts are tasked with providing technical expertise to analyse algorithms, identify and manage systemic risks posed by very large online platforms and very large online search engines, and study the long-term societal impact of algorithms.

5. See the presentation of the Artificial Intelligence Act included in the section "Artificial Intelligence and Intelligence Gathering" in the 8th CNCTR Activity Report for 2023.

6. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Regulation).

7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for digital services and amending Directive 2000/31/EC.

8. Acronym referring to Google (and the Alphabet group to which it belongs), Apple, Facebook (and the Meta group), Amazon, and Microsoft.

Legislation on data control: the Data Act, the Data Governance Act[9], and the GDPR[10]

The Data Governance Act and the Data Act on harmonised rules for fair access and use of data aim to strengthen the EU's competitiveness and sovereignty in data governance by establishing a harmonised framework enabling economic operators and EU Member States to harness the potential of data and foster innovation. These texts therefore aim to promote access to, sharing and reuse of data in Europe, in accordance with EU law – in particular the rules on personal data protection laid down in the General Data Protection Regulation (GDPR). The latter aims to give European residents greater control over their personal data by regulating the automated processing to which it may be subject. It incorporates and expands upon the key principles already established in European law and the French Data Protection Act of 6 January 1978, notably the right to access personal data, the rights to rectify and erase one's data, and the ability to request delisting.

As soon as they process or use data, algorithms must comply with this legislation.

Cybersecurity legislation: the Network and Information Security 2 (NIS 2) Directive[11]

The Directive on the security of networks and information systems (known as NIS 2) aims to raise the overall level of cybersecurity in Europe by applying a harmonised and simplified framework setting rules for strengthening cybersecurity measures, incident management and the supervision of entities providing services that are essential for the maintenance of critical social or economic activities. It is specified and supplemented by three European regulations: the regulation concerning ENISA and the cybersecurity certification of information and communication technologies, known as

9. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Regulation], and Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act).

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

the Cybersecurity Act; the regulation on horizontal cybersecurity requirements applicable to products with digital components, called the Cyber Resilience Act (CRA); and the regulation establishing measures to strengthen solidarity and capabilities within the Union to detect, prepare for, and respond to cybersecurity threats and incidents, referred to as the Cyber Solidarity Act.

This study aims, while respecting national defence secrecy, to set out the legal and technical reality (1). In this way, the spectre of a mass surveillance tool can be dispelled by describing a rigorously controlled threat detection technique (2).

1. From the spectre of a mass surveillance tool...

1.1. The origins of the legal framework: the path of experimentation in response to a feared technique

1.1.1. A limited but necessary exception to the principle of targeted and individualised surveillance

The legal framework established by Book VIII of the French Internal Security Code on intelligence is built around the cardinal principle set out in its introductory article, according to which "***Respect for privacy, in all its aspects, including the secrecy of correspondence, the protection of personal data and the inviolability of the home, is guaranteed by law***" (see Article L. 801-1).

To ensure compliance with this principle, the legislator has opted for the individualisation of surveillance carried out on the **national territory or targeting technical identifiers, such as telephone numbers or email addresses, that can be linked to the national territory**. The intelligence-gathering techniques provided for by law in this area refer to tools designed to place a specific individual or their

attributes (vehicle, home, identifiers, correspondence or words, etc.) under surveillance. In parallel, Article L. 821-2 of the French Internal Security Code requires that when an intelligence service requests authorisation to implement an intelligence-gathering technique, it must specify not only the purposes and grounds for the surveillance but also the person or persons targeted by the technique. This person may, of course, be identified or not, may, for certain techniques, belong to the entourage[12] of the primary target, or in rare situations, which are particularly closely monitored by the commission, may be a legal entity or an informal entity without legal personality. Nevertheless, the entire legal framework governing intelligence in France is built around the individual and targeted use of domestic surveillance techniques, in clear contrast to the approach of mass surveillance adopted by certain other states.

A fundamental and structuring application of the principle of proportionality in surveillance, as established by the 2015 legislator, the individual targeting of intelligence-gathering techniques reflects the choice to limit the collection of information to what is strictly necessary. This approach is in stark contrast to the American option, which allows intelligence services to intercept and store massive amounts of data on residents and non-residents[13], whose extensive

12. See on this point the thematic factsheet "The entourage of surveilled individuals" available on the CNCTR website, as well as the study "Surveilling the entourage?" in the 8th CNCTR Activity Report for 2023, p. 117 et seq.

13. Mass surveillance in the United States: from the USTO programme to the Patriot Act.
The USTO programme: the "US to other countries" programme, known as "USTO", established in 1992, is often presented as the first American mass telecommunications surveillance programme. It required all telephone operators to provide a list of all calls from the United States to countries that might be involved in drug trafficking.
Under this programme, endorsed by the US Department of Justice, surveillance of the communications of US citizens and nationals of 116 countries was reportedly set up for the benefit of the Drug Enforcement Administration (DEA), the agency responsible for combating drug trafficking. The programme was officially terminated in 2013, following revelations by Edward Snowden.
FISA and the Patriot Act:
Since the post-war period, and particularly in the context of the Cold War, the United States has continuously developed its communications interception capabilities, particularly within the framework of post-war intelligence partnerships between allies.
In terms of exploitation, US surveillance systems were significantly strengthened following the attacks of 11 September 2001, with, in particular, the adoption the following month of the USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), a law that expanded the powers of the National Security Agency (NSA) and other intelligence and investigative agencies (particularly the FBI and CIA) by facilitating the requisition of domestic surveillance data. The agencies now have broader powers to obtain personal information about users from telecommunications operators and to archive and exploit large amounts of data obtained through electronic surveillance for preventive purposes. A few years later, a new provision adopted in 2008 further legalised surveillance techniques secretly authorised by the White House after the attacks. Section 702 of the Foreign Intelligence Surveillance Act (FISA) of 1978 has since authorised intelligence agencies to collect data on citizens and companies located outside the United States, giving US surveillance mechanisms a particularly wide scope.
While some of the emergency measures adopted in response to the 2001 attacks have been revised or abolished, notably the highly controversial programme for the storage and use of Americans' telephone and computer metadata authorised for preventive purposes by Section 215 of the Patriot Act, most of the domestic and international mass surveillance mechanisms both domestic and international, remain firmly entrenched in the US legislative landscape.
See in particular Report No. 2697 of 2 April 2015 by Mr Jean-Jacques Urvoas on behalf of the Committee on Constitutional Law, Legislation and General Administration of the National Assembly, as well as the hearing of the ministers before the National Assembly on 31 March 2015.

practice was revealed in June 2013 by Edward Snowden, a former consultant to the National Security Agency (NSA), who disclosed the existence of programmes for the systematic collection of metadata from telephone calls made in the United States or from the United States to other countries. As reflected in the parliamentary debates of the time, **the French legislator clearly intended to reject the establishment of *"indiscriminate mass surveillance"*** by intelligence services, of the kind that could be carried out, as in the United States, ***"with no real limitation other than that imposed by technological constraints"***, a difference in approach illustrated by the image of France's "harpoon fishing" method as opposed to America's "trawler fishing" model.

In France, only the surveillance of international electronic communications, when not intended to track identifiers linked to the national territory, is exempt from this rule. The difference in approach compared to domestic surveillance stems from the fact that, since persons located abroad are outside the jurisdiction of the State and cannot, in particular, be subject to binding legal measures based on the information collected, the interception of their communications is not likely to infringe their rights to the same extent as if they were located on national territory[14].

THE SPECIFIC NATURE OF INTERNATIONAL SURVEILLANCE

Despite the disappearance of physical borders in the digital world, intelligence law remains marked by the principle of territoriality.

The surveillance of international electronic communications, whether correspondence or internet connection data, is thus governed by a specific chapter of Title V of Book VIII on intelligence in the French Internal Security Code.

14. See the Government's observations on Decision No. 2015-722 DC of 26 November 2015 of the Constitutional Council and the study by the Council of State entitled "Digital technology and fundamental rights" - 2014.

The provisions of Articles L. 854-1 to L. 854-9 of the French Internal Security Code, which make up this chapter, provide that intelligence services may be authorised to exploit communications sent or received abroad on electronic communications networks designated by the Prime Minister. Unlike techniques implemented on national territory or relating to a technical identifier linked to national territory, which are subject to individualised and targeted surveillance, international electronic communications may be monitored by means of non-individualised authorisations targeting geographical areas, organisations or groups (see point 3 of Article L. 854-2 III).[15]

The need to give the services adequate and proportionate means of action to prevent threats has led to the introduction of an exception to the principle of targeted and individualised surveillance.

Two major constraints have led the legislator to allow a departure from this principle.

The intensification and diversification of threats since the beginning of the century, marked in particular by the rise of a global terrorist movement made up of countless cells and isolated individuals, has made it necessary to use surveillance methods capable of detecting this diffuse and evolving threat, which includes individuals with no apparent links to organised groups, networks, or structured entities.

Furthermore, the exponential growth in data production accompanying the rise of digital technologies, such as the development of secure exchange networks, has revealed the limitations of traditional surveillance tools, which are powerless to detect offences and threats in the massive and constant flow of data circulating in the digital space.

Aware of these challenges, the legislator wanted to give French intelligence services the option of implementing algorithmic processing to detect terrorist threats, without identifying people involved in the analysis

15. See on this point the presentation "Surveillance of international electronic communications" available on the CNCTR website.

of data other than those suspected of terrorism. The aim was therefore to cross-check and analyse a large number of technical elements in order to detect low-intensity signals suggesting a terrorist threat, without resorting to mass surveillance, i.e. without conceding any "collateral damage" to individual freedoms.

It is essential to clarify that the dataset on which the algorithm operates is not made available to the services; only the small portions corresponding to positive detection results are provided to them.

1.1.2. The introduction on an experimental basis of the algorithmic technique by the Act of 24 July 2015

The Intelligence Act of 24 July 2015 established a specific use of algorithms, as an intelligence-gathering technique in their own right, solely for the purposes of preventing terrorism. To this end, Article 5, reproduced in Article L. 851-3 of the French Internal Security Code, authorised the use of algorithmic processing techniques, commonly referred to as "algorithms", on data from electronic communications operators and internet service providers in order to detect connections that may reveal a terrorist threat.

The algorithms governed by Article L. 851-3 of the French Internal Security Code thus became, in 2015, the second category of algorithmic processing authorised by law on mass data for public security purposes, alongside those introduced in 2013 for the analysis of personal data collected during international travel, provided for in Article L. 232-7 of the same code[16].

16. API-PNR system relating to passenger check-in and booking data.

AN INTELLIGENCE-GATHERING TECHNIQUE VALIDATED BY THE CONSTITUTIONAL COUNCIL

When reviewing the Intelligence Act, the Constitutional Council ruled that the provisions of Article L. 851-3 of the French Internal Security Code concerning algorithmic processing were consistent with the Constitution[17]17, judging that they did not constitute a manifestly disproportionate infringement of the right to respect for private life.

The Council specifically noted that "*both the use of the technique and the parameters of the automated processing are authorised following an opinion from the National Oversight Commission for Intelligence-Gathering Techniques*", that the automated processing, intended to detect terrorist threats, uses only connection data "*without collecting data beyond what is defined by the system's design parameters and without identifying the individuals to whom the information or documents relate,*" and finally, "*when data detected through automated processing is likely to indicate a terrorist threat, a new authorisation from the Prime Minister is required, after an opinion from the National Oversight Commission for Intelligence-Gathering Techniques, in order to identify the individual concerned (...).*"

As a sign of its caution regarding this new, innovative and complex surveillance tool, the legislator opted for a trial system, with its use initially authorised for only three years, until 31 December 2018.

However, this deadline was extended twice, prolonging the trial until 31 December 2021.

The first extension became necessary due to the difficulties encountered in developing the new algorithm-based technique, combined with the strict oversight exercised by the CNCTR throughout this trial. After a phase of study and examination of possible options conducted by the Inter-Ministerial Control Group (GIC),

17. See Decision No. 2015-713 DC of 23 July 2015 of the Constitutional Council, §58 et seq.

in conjunction with the Directorate-General for Internal Security (DGSI) and the Directorate-General for External Security (DGSE), the general architecture project selected for the implementation of automated processing was not finalised until spring 2017 by a classified decision of the Prime Minister on 27 April, the initial drafts having been revised to take into account the observations and recommendations made by the CNCTR concerning, in particular, the conditions for data storage and access[18]. After validation of the general technical framework, additional studies were necessary to build the first algorithm, in particular to determine the alert parameters likely to indicate a terrorist threat and to select the data to be processed in order to build an operational, relevant and proportionate system. The complexity of this preparatory work explains why the initial implementation of an algorithm was not finally authorised by the Prime Minister until 12 October 2017[19], following favourable opinions issued by the CNCTR plenary session in two classified deliberations on 26 July and 5 October 2017.

Given the limited time available to assess the operational benefits of the algorithms, which were effectively implemented at the end of 2017, the trial was extended until 31 December 2020 by Article 17 of law no. 2017-1510 of 30 October 2017 strengthening internal security and the fight against terrorism, known as the SILT Law.

A second extension of the trial period was introduced by Article 2 of law no. 2020-1671 of 24 December 2020, to take into account the impact of the health crisis caused by the COVID-19 epidemic on government work and the parliamentary timetable, which made it difficult for Parliament to examine, in due time and under appropriate conditions for debate, whether to make permanent or discontinue the new surveillance tool based on automated processing.

18. For a detailed description of the design of the technical architecture of the algorithms, see the 2nd activity report for 2017 of the CNCTR, p. 16 et seq.

19. See the CNCTR's 2020 activity report, p. 16 et seq.

ANOTHER EXAMPLE OF RESERVATIONS ABOUT THE USE OF ALGORITHMS IN PUBLIC ORDER MATTERS, BUT OUTSIDE THE REMIT OF THE INTELLIGENCE SERVICES, IS SO-CALLED "AUGMENTED" OR "INTELLIGENT" VIDEO SURVEILLANCE

Outside the scope of the intelligence services, the deployment in public places of "augmented" camera or video devices, i.e. image recording devices linked to algorithmic processing software that enables automatic analysis of the data captured in order, for example, to detect shapes or objects, analyse movements, or identify behaviour contrary to public order or offences, has been the subject of heated debate in recent years.

The new challenges raised by the increasingly widespread use of video technology based on artificial intelligence, particularly by public authorities in so-called "safe city" projects launched in Nice, Marseille and Saint-Etienne, have been highlighted by independent administrative authorities, associations and academics, calling for strict regulation of the various uses. The French Data Protection Authority (CNIL) has highlighted the change in the nature of algorithmic video surveillance compared to traditional cameras that film live and record video sequences viewed by a human operator. The proliferation of the system's capabilities and the massive processing of personal data pose a particular risk to individual and collective rights and freedoms, leading to an increased risk of widespread surveillance[20].

The most controversial use of these systems is undoubtedly algorithmic video surveillance in the field of public safety. This is evidenced by the parliamentary debates that preceded the adoption of Article 10 of law no. 2023-380 on the 2024 Olympic and Paralympic Games, authorising the experimental use of augmented video surveillance using fixed cameras or drones for the security of sporting, recreational and cultural events.

20. See in particular the CNIL's position on so-called smart or augmented cameras in public spaces, published on 19 July 2022.

As with the algorithm technique provided for in Article L. 851-3 of the French Internal Security Code, the legislator has adopted a cautious approach based on experimentation, with the use of algorithmic video surveillance only authorised until 31 March 2025. It also strictly regulated the use of this tool, both in terms of its purposes and its implementation conditions, authorising only the detection of anomalies or specifically defined risk situations, and prohibiting the use of any process that could enable the identification of an individual.

The report of the evaluation committee on this trial[21], submitted in January 2025 to Parliament and the CNIL, highlights the benefits of algorithmic video surveillance in terms of security, while also presenting the concerns and reservations expressed by the public and organisations involved in defending rights and freedoms, particularly regarding the risk of a ratchet effect, whereby the adoption of more intrusive new technology could lead to the normalisation of general surveillance based on AI.

1.2. The permanent adoption and extension of the technique recognised as necessary, but cautiously accepted

1.2.1. The undeniable benefits of the technology have led to its permanent adoption, accompanied, however, by new safeguards

Without waiting for the deadline given to the government to submit a report to Parliament on the testing of the algorithm technique, set most recently for 30 June 2021, several public intelligence policy

21. Report of the evaluation committee on the trial of algorithmic processing of images legally collected by means of video protection systems.

actors have spoken out on the contributions of the automated processing implemented.

Highlighting the terrorist threat, the rapporteurs of the National Assembly's fact-finding mission on the evaluation of the law of 24 July 2015[22] emphasised, as early as summer 2020, the need to extend the use of the algorithm, as they considered this technique to meet an operational need. Despite relatively limited implementation, with only three algorithmic processes in place and operational at the beginning of 2020, the mission concluded that the results were interesting and even suggested ways of improving the effectiveness of a system that was already promising.

Similarly, the CNCTR ruled in favour of continuing algorithmic surveillance, justified by the reality of a persistent and diffuse terrorist threat. It recognised the contribution of this detection tool, which is the only one in the arsenal of techniques authorised by the French Internal Security Code that is capable of identifying isolated individuals whose dangerous potential can sometimes only be revealed through their digital activity[23]. The assessment of the use of the technique, set out in a classified government report dated 30 June 2020 for the Parliamentary Intelligence Committee (DPR) and the commission, appeared sufficiently convincing to recommend the permanent adoption of the system provided for in Article L. 851-3 of the French Internal Security Code, the trial of which involved close participation from the commission[24]

Without disclosing the elements of this report, which are covered by national defence secrecy, the government presented general information on the conduct of the trial and the operational

22. See information report no. 3069 submitted on 10 June 2020 by the joint information mission of the Law Commission/ Defence Commission of the National Assembly on the evaluation of the Intelligence Act of 24 July 2015 and presented by Mr Guillaume Larrivé, Chairman, Mr Loïc Kervran and Mr Jean-Michel Mis, rapporteurs.

23. See CNCTR deliberation no. 2/2021 of 7 April 2021, available on the website. https://cms.cnctr.fr/uploads/NP_CNCTR_2021_deliberation_2_2021_04_07_d5f3cf8590.pdf?updated_at=2023-04- 21T16:27:30.844Z

24. See the minutes of the closed hearing of Wednesday 12 May 2021 before the National Defence and Armed Forces Committee of the National Assembly of Mr Francis Delon, Chairman of the CNCTR.

effectiveness of the technique in the impact assessment of 11 May 2021 on the draft law on the prevention of terrorist acts and intelligence, which proposed making the provisions relating to the algorithm permanent. On this last point, the study indicates that the system "***is essential for detecting individuals unknown to the intelligence services or whose previous behaviour had not previously allowed them to be identified as threatening***", specifying that the algorithms in operation have in particular made it possible to "***identify individuals posing a terrorist threat and detect contacts between individuals posing a threat; obtain information on the location of individuals linked to this threat; update the behaviour of individuals known to the intelligence services and requiring further investigation; improve the services' knowledge of how individuals in the terrorist movement operate***". The government concluded that the algorithm technique meets an essential need for the early detection of terrorist threats, noting, on the one hand, that it makes it possible to identify "***a new threat, whose perpetrators and methods are unknown and therefore cannot, by definition, be subject to prior targeted surveillance***", and on the other hand, that it is a tool suited to the development of new digital behaviours, "***particularly given the widespread online dissemination of terrorist propaganda and the emergence of new electronic communications channels***[25]".

In view of these factors, law no. 2021-998 of 30 July 2021 on the prevention of terrorist acts and intelligence, known as the "PATR" law, has made the use of algorithms permanent. Nevertheless, mindful of containing its use and limiting its potential impact on rights and freedoms, the legislator accompanied the permanent adoption of this technique with new safeguards, mainly by restricting the intelligence services authorised to request its use and by granting the GIC exclusive authority to carry out the authorised processing on behalf of those services (see point 2.1.2 below). In addition, the law amended the rules governing requests for authorisation to use

25. Explanatory memorandum to the draft law on the prevention of terrorist acts and intelligence.

intelligence-gathering techniques, including algorithms, by making the prior opinion of the CNCTR highly binding[26], thereby ensuring that requests comply with the requirements of European Union law.

1.2.2.| ... and a cautious extension of its scope of use

Another sign of the interest generated by algorithms is that their scope has been extended, first in terms of the data that can be subject to automated processing in the wake of their permanent adoption, and subsequently in terms of the purposes for which they can be used.

Initially limited to processing connection data only, the need to extend the use of algorithms to cover complete internet resource addresses, or URLs[27], was raised in the two aforementioned reports issued in June 2020. The overly narrow scope of the data that could be analysed in the automated processing trial was deemed partly responsible for the tool's limited results.

The evolution of the terrorist threat, now embodied by a myriad of individuals inspired by jihadist propaganda messages or incitement to action by terrorist organisations or radicalised groups disseminated on the internet, makes it particularly useful, from an operational point of view, to collect URLs that enable more accurate identification of digital activities involving the consultation of websites relaying this type of content.

The extension of the algorithm technique to the analysis of all information contained in URLs, which in effect amounts to authorising the automated processing of data that partly reflects the content of communications, has therefore become necessary for the services responsible for combating terrorism.

26. See the provisions of Article L. 821-1 of the French Internal Security Code, as amended by Article 18 of the Law of 30 July 2021.
27. See box below, p 160.

The recognition of this operational need by the various public authorities responsible for intelligence, in particular the CNCTR[28], has led to the scope of data that can be analysed using algorithmic techniques being extended to include the full addresses of resources used on the internet, as specified in Article L. 851-3 of the French Internal Security Code since the entry into force of the aforementioned PATR law.

Here again, the legislator's cautious approach to this significant development of the technique resulted in the government being required to submit a report to Parliament on the application of Article L. 851-3 of the French Internal Security Code by no later than 31 July 2024[29], to ensure that the intrusion into private life is genuinely justified by improved protection against the terrorist threat. This expansion of the scope of technical investigation has also been accompanied by adjustments to the data regime to limit the storage of processed data to what is strictly necessary (see point 2.1.2. below).

CONNECTION DATA, CONTENT DATA, URL ADDRESSES

In the field of digital data processing, the French Internal Security Code distinguishes between connection data and content data. Thus, Article R. 851-5 lists the connection data that may be collected, specifying that the relevant information and documents are gathered "*to the exclusion of the content of the correspondence exchanged or the information consulted (...)*". This distinction is in line with that made by Article L. 34-1 of the French Postal and Electronic Communications Code, which sets out the data relating to electronic communications that operators are required to retain, specifying that such data "*relates exclusively to the identification of users of the services provided by operators, the technical characteristics of the communications provided by them and the location of terminal equipment [but] may not in any case relate to the content of correspondence exchanged or information consulted, in any form whatsoever, in the context of such communications*."

28. See CNCTR deliberation no. 2/2021 of 7 April 2021, available on its website.
29. This obligation is set out in Article 15(II) of the aforementioned PATR law of 30 July 2021.

Internet connection data, as opposed to the content of correspondence exchanged or information consulted, refers to the "container", i.e. the data enabling the transmission of electronic communications.

However, the classification to be used is not clear for certain technical elements such as website or web page addresses, known as URLs. The URL, short for Uniform Resource Locator, is an alphanumeric string that specifies the location of an internet resource by indicating the type of protocol to be used to access it (such as http or https for a web page). Its structure, which includes the domain name of the server or its IP address and the access path to the resource, specifies the page the user wishes to consult, along with, where applicable, other data completing the request. It therefore identifies the address of content, without constituting the content itself.

For both the CNCTR and the CNIL[30], URLs are considered "mixed data", comprising both connection data, relating to the transmission of the internet communication, and content data, in so far as they provide details about the purpose or content of the website visited. Based on this dual nature of URLs, the CNCTR considered that administrative access to internet connection data provided for in Article L. 851-1 of the French Internal Security Code could only allow, in the case of URLs, the collection of parts of URLs determining the path used to exchange correspondence or consult information, with other elements being eliminated[31].

The aforementioned PATR law of 30 July 2021 formally recognises the mixed nature of URLs, treating them as a sui generis category of data. Since its adoption, the French Internal Security Code has specified that the relevant techniques provided for in Articles L. 851-2 (real-time access to technical connection data) and L. 851-3 (algorithm) may apply not only to the connection data referred to in Article L. 851-1 but also to "the complete addresses of internet resources."

30. CNIL Decision No. 2015-455 of 17 December 2015 on a draft decree of the Council of State on intelligence-gathering techniques (referral No. 15033364).

31. Deliberation No. 1/2016 of 14 January 2016 on the terms and conditions for the application of Article L. 851-1 of the French Internal Security Code, available on the CNCTR website.

In addition, the scope of use of the algorithm has been extended to two new purposes.

As soon as the first results of the trial of the technique became available, calls were made to extend its use to purposes other than the prevention of terrorism, citing in particular the usefulness of this tool in cyber defence, counter-espionage and, more recently, organised crime[32]. In light of the results presented in relation to terrorism prevention, the usefulness of the technique for detecting, for example, foreign services' manoeuvres or malicious attacks has thus been highlighted.

Taking these recommendations into account concerning counter-espionage and counter-interference, law no. 2024-850 of 25 July 2024 on the prevention of foreign interference and threats to national defence authorised the use of the algorithm to protect and promote national independence, territorial integrity, and national defence (purpose mentioned under point 1 of Article L. 811-3 of the French Internal Security Code), as well as to safeguard major interests of France's foreign policy, ensure compliance with France's European and international commitments, and prevent all forms of foreign interference (purpose mentioned under point 2 of the same Article L. 811-3), for the purposes of "***detecting foreign interference***" and "***threats to national defence***".

Nevertheless, renewing its cautious approach, the legislature authorised the extension of the algorithm to these new purposes only on a trial basis, for a period of three years, until 1 July 2028. This period is intended to allow the services to demonstrate the real added value of the technique in enhancing the detection of any form of foreign interference or any threat to national defence[33].

In addition, enhanced parliamentary control over this new trial has been established by Article 6(III) of the law, requiring the government to

32. See Information Report No. 3069, submitted on 10 June 2020 by the joint information mission of the Law Commission and the Defence Commission of the National Assembly on the evaluation of Intelligence Act of 24 July 2015, presented by Mr Guillaume Larrivé (Chair), Mr Loïc Kervran and Mr Jean-Michel Mis (rapporteurs), as well as the 2022–2023 activity report of the Parliamentary Intelligence Committee, which recommended trialling the extension of the algorithm to the purposes mentioned under points 1 and 2 of Article L. 811-3 of the French Internal Security Code.

33. The law aimed at freeing France from the trap of drug trafficking, adopted on 28 and 29 April by Parliament, nevertheless includes a provision to postpone this date to 31 December 2028. This text was the subject of three referrals to the Constitutional Council on 12 May 2025. At the time of finalisation of this report, the Constitutional Council had not yet issued its decision.

submit two reports. An initial assessment report must be submitted by 1 July 2026 at the latest, followed by a second report on the results of the technology for the new purposes set out, which must be submitted to Parliament no later than six months before the end of the trial period. These two reports must also be submitted to the Parliamentary Intelligence Committee (DPR) in a classified version including examples of the implementation of the algorithms.

A NEW EXTENSION OF THE PURPOSE OF THE ALGORITHM? THE BILL AIMED AT FREEING FRANCE FROM THE TRAP OF DRUG TRAFFICKING:

Submitted on 7 May 2024, report no. 588, "*A necessary wake-up call: escaping the trap of drug trafficking*" by the Senate commission of inquiry chaired by Mr Jérôme Durain recommends, in view of the impact of drug trafficking on France, "*a shock treatment to end the impunity enjoyed by traffickers at the top of the spectrum (...) and to restore each actor to their rightful role in the fight against drug trafficking*". With this in mind, the report examines the potential of algorithmic intelligence, proposing to consider extending this intelligence-gathering technique to the fight against drug trafficking in an ad hoc experimental framework that precisely defines the cases of organised crime that justify its use (recommendation 20).

Based in particular on this report, the bill aimed at freeing France from the trap of drug trafficking, tabled in the Senate on 12 July 2024, seeks to provide the services responsible for preventing organised crime and delinquency with new means of tracking drug traffickers who are skilled at evading traditional surveillance capabilities.

In the version adopted by Parliament on 28 and 29 April 2025, the text thus provides for extending the trial of the algorithm, provided for by the law of 25 July 2024, to the purpose mentioned in point 6 of Article L. 811-3 of the French Internal Security Code, and also postpones its expiry date to 31 December 2028[34].

34. The text adopted by Parliament has been referred to the Constitutional Council on three occasions. At the time of finalisation of this report, the Constitutional Council had not yet issued its decision.

2. … to the deployment of a threat detection technique, subject to rigorous oversight

2.1. Strict oversight of a threat detection technique

2.1.1. The operating principles of the algorithm: the link between detection and surveillance, authorisation at each stage

To present the automated processing systems introduced by the law of 24 July 2015, the rapporteurs of the joint information mission of the National Assembly's Law and Defence Committees evaluating that law called for efforts to "***demystify the algorithm***, [which] ***is not a mass surveillance tool, but rather a means of detecting weak signals that may subsequently justify the use of an intelligence-gathering technique, within the framework of ordinary law***"[35].

In the architecture adopted by the French legislature, the algorithm was designed as a tool for detecting, based on predetermined parameters subject to prior control, weak signals that could reveal a threat to the fundamental interests of the nation, while minimising infringements of individual freedoms. Thus, the technique does not in any way allow intelligence services to access and analyse all the data on operators' networks. On the contrary, the system is designed to discriminate as precisely as possible, within that data, those elements likely to reveal a threat, in order to guide the surveillance work of the services and, where appropriate, to enable targeted, individual monitoring limited to what is strictly necessary.

35. See information report no. 3069 submitted on 10 June 2020 by the joint information mission of the Law Commission/ Defence Commission of the National Assembly on the evaluation of the Intelligence Act of 24 July 2015 and presented by Mr Guillaume Larrivé, Chairman, Mr Loïc Kervran and Mr Jean-Michel Mis, rapporteurs.

This intelligence-gathering technique operates in two stages. First, the algorithmic processing analyses data flows according to parameters pre-established at the time of its design in order to detect activity that is suspicious in relation to the intended purpose, without the intelligence services being able to access these flows directly. Only if, and only when, the algorithmic processing detects activity that meets its design criteria ("hit") are the intelligence services alerted and can, in a second stage, access only the data corresponding to this "hit" and the identification of the persons to whom it relates, by making a request for the anonymisation to be lifted.

The procedure put in place can be summarised as follows: after the requesting service has obtained authorisation to use an algorithm to detect connections that may reveal a threat, the corresponding automated processing is carried out by the GIC. When this processing triggers an alert, the GIC notifies the service authorised to implement the algorithm of this "hit", without this notification containing or revealing the data that triggered it. On the basis of this minimal information, the service may request access to the data that triggered the alert and the identification of the people involved by submitting a request for the anonymisation to be lifted, subject to the prior opinion of the CNCTR and then the authorisation of the Prime Minister.

If this authorisation is obtained, the GIC gathers the data and communicates it to the service. Thus, no intelligence service can access the data subjected to automated processing. The only data that may be passed on to them are those that triggered an alert from an algorithm authorised by an initial decision of the Prime Minister, and whose anonymity has subsequently been lifted by a new decision of the Prime Minister.

Three steps are therefore required for the algorithmic technique to result in the surveillance of an individual, with each stage requiring authorisation from the Prime Minister, who decides after

receiving the CNCTR's opinion on the substantiated request from the relevant intelligence service:

- an initial authorisation to implement automated processing, issued pursuant to Article L. 851-3 of the French Internal Security Code,
- a second authorisation to lift the anonymity of the person detected by the processing, issued pursuant to IV of the same article,
- finally, where applicable, authorisation to use an intelligence-gathering technique targeting that person (obtaining internet connection data; security interceptions; etc.).

The algorithmic technique provided for by the French Internal Security Code cannot therefore be equated, in terms of its purpose, structure or legal operation, with an instrument for the general surveillance of information or communications exchanged by individuals in the digital sphere.

PRINCIPLES OF DETECTION SET OUT IN ARTICLE L. 851-3 OF THE FRENCH INTERNAL SECURITY CODE

"I. (...) for the sole purposes provided for in points 1, 2 and 4 of Article L. 811-3, at the request of the specialised intelligence services mentioned in Article L. 811-2, automated processing may be authorised, based on the data transiting through the networks of the operators and persons mentioned in Article L. 851-1, in order to detect, according to parameters specified in the authorisation, connections likely to reveal foreign interference, threats to national defence or terrorist threats.

Such automated processing shall use only the information or documents referred to in Article L. 851-1 and the full addresses of resources used on the internet, without collecting any data other than those that meet their design parameters and without allowing the identification of the persons to whom the information, documents or addresses relate. / (...)

In accordance with the principle of proportionality, the Prime Minister's authorisation specifies the technical scope of the implementation of this processing.

II.- The National Oversight Commission for Intelligence-Gathering Techniques shall issue an opinion on the request for authorisation relating to automated processing and the detection parameters selected. (...)

IV - When the processing (...) detects data likely to characterise the existence of a threat, the Prime Minister (...) may authorise the identification of the person or persons concerned and the collection of related data, after obtaining the opinion of the National Oversight Commission for Intelligence-Gathering Techniques (...). (...) ".

2.1.2. | A very strict legal and technical framework

Although the algorithm was designed as an advanced threat detection tool, its integration into the standard legal framework for intelligence has generated significant concerns due to the potential risks linked to the automated processing on which the technique relies. The use of such systems inherently carries risks of infringing rights and freedoms, particularly the right to privacy and the protection of personal data, simply because they enable the mass processing and analysis of digital data.

These concerns, which continue to echo in major public debates about the ability to explain artificial intelligence results and the concept of trustworthy AI, justify the particularly strict legal framework governing the use of algorithms. Apart from the recent broadening of its scope (see above), this framework has, in fact, been further strengthened over time.

It should first be noted that the use of automated processing is subject to a stricter authorisation regime than that applied to other intelligence-gathering techniques, pursuant to the provisions of Article L. 851-3 of the French Internal Security Code:

- the algorithm may only be authorised for the purpose of detecting connections that may reveal foreign interference, threats to national defence or terrorist threats. To date, it can therefore only be based on **three purposes**[36] out of the eight provided for in Articles L. 811-3 and L. 855-1 of the French Internal Security Code;

36. The bill aimed at freeing France from the trap of drug trafficking, adopted by Parliament on 28 and 29 April 2025, provides for an extension of the technique to the purpose mentioned in point 6 of Article L. 811-3 of the French Internal Security Code. Its provisions are, however, the subject of three referrals to the Constitutional Council dated 12 May 2025 (Referrals 2025-885 DC). At the time of finalisation of this report, the Constitutional Council had not yet issued its decision.

- only the six specialised intelligence services, known as **first circle services**, are authorised to use it;

- the two-stage operation of the technique requires the services to obtain **two successive authorisations** from the Prime Minister, each after consultation with the CNCTR, relating to the implementation of automated processing and then to the lifting of anonymity in the event of a threat being detected;

- the initial authorisation to implement automated processing is limited to **two months**, and, if it is renewable for four months under the conditions of ordinary law, the request for renewal must be accompanied by **specific reasons** including, in addition to the information provided for in Article L. 821-2 of the French Internal Security Code[37], a statement of the number of identifiers reported by the automated processing and an analysis of the relevance of these reports;

- finally, **the urgency** allowing the Prime Minister to order the immediate implementation of a technique in the event of an unfavourable opinion from the CNCTR, as provided for in Article L. 821-1 of the French Internal Security Code, cannot be invoked for the implementation or renewal of an algorithm.

In addition, enhanced safeguards were initially provided for or added in order to limit the intrusive nature of the technique:

- with regard to **processed data**, while automated processing was extended to URLs in 2021, this extension of the scope of the technique was accompanied by an adjustment of

37. Article L. 821-2 of the French Internal Security Code provides that requests for intelligence-gathering techniques must specify: *"1. The technique or techniques to be implemented; 2. The service for which it is being requested; 3. The purpose or purposes pursued; 4. The grounds for the measures; 5. The period of validity of the authorisation; 6. The person or persons, places or vehicles concerned.*
For the purposes of point 6, persons whose identity is not known may be designated by their identifiers or their status, and the places or vehicles may be designated by reference to the persons who are the subject of the request.
Where the purpose of the request is to renew an authorisation, it shall state the reasons why such renewal is justified in relation to the purpose or purposes pursued."

the regime for all data covered by the algorithm in order to limit as far as possible any infringement of freedoms. Data detected as likely to indicate the existence of a threat in the context of an alert may only be retained for sixty days, without the possibility of extending this period of use to four years as provided for during the trial period. In addition, the law now requires that data not detected by processing as likely to reveal a threat must be destroyed immediately.

- furthermore, because automated processing can potentially be very intrusive, it is necessary to carry out **a rigorous assessment of the proportionality** between the interference with privacy and personal data and the protection of the fundamental interests of the nation, specific mechanisms for **algorithm control** are provided for. In addition to the parliamentary evaluations and controls imposed in the context of the above-mentioned trials, the French Internal Security Code takes care to confer on the CNCTR the necessary prerogatives for the proper exercise of its oversight of this innovative and complex technology. Pursuant to Article L. 851-3(II) of this code, **the commission must therefore have "*permanent, complete and direct access to such processing and to the information and data collected*"**, and it must be "***informed of any changes made to the processing and parameters***". In addition, the commission has the power to issue recommendations on the algorithm's technique, in addition to the general power it has under Article L. 833-6 of the same code.

Finally, the framework for the algorithm also covers the technical system enabling its implementation, which has been redesigned to be more protective.

The permanent adoption of the technique was accompanied by the incorporation into legislation of the technical and organisational

architecture established in 2017, assigning responsibility for the centralised execution of algorithms to the GIC.

The technical architecture for implementing the algorithms resulted from coordinated efforts by the services of the Prime Minister, the GIC, and the CNCTR during the design of the first algorithm's operational system in 2016–2017. These efforts sought to strike a balance between the effectiveness of the technique and limiting infringements on privacy and the confidentiality of communications to the strict minimum.

During discussions on the Intelligence Act in 2015, an option had been considered whereby operators themselves would execute the automated processing by installing detection devices at multiple points across their networks. However, this implementation method was abandoned in light of its practical disadvantages (risks to the security of these networks, reduced detection capability due to the fragmentation of networks, and the exposure of detection parameters[38] to the operators). Consequently, the government opted for a centralised implementation of the algorithms, consisting of duplicating the internet connection data flows on the operators' networks and then routing them to the GIC, which is responsible for carrying out all the automated processing provided for in Article L. 851-3 of the French Internal Security Code.

When consulted on an initial draft general architecture incorporating this principle, the CNCTR made several recommendations in a classified deliberation, including one recommending that the centralised system be placed under the sole and entire responsibility of the GIC. Acting as a screen between the data analysed by the algorithms and the intelligence services that requested their implementation, this centralisation within the GIC appeared to be an essential technical safeguard to ensure that

38. See impact assessment on the draft law on the prevention of terrorist acts and intelligence, 11 May 2021: https://www.assemblee-nationale.fr/dyn/15/textes/l15b4104_etude-impact.pdf.

the intelligence services could not at any time directly access the data subject to automated processing. Correlatively, the commission recommended the establishment of a system for tracing all access to the system, in order to control its security *vis-à-vis* the intelligence services and, more broadly, any agent other than those individually authorised to intervene in the execution of automated processing. Finally, the CNCTR recommended that a very short storage period be set for data subject to automated processing within the GIC, limited to the time strictly necessary to enable the algorithms to be executed.

Taking all these observations and recommendations into account, the Prime Minister laid down the general rules for the implementation of algorithms in a classified decision of 27 April 2017. Section VI of Article L. 851-3 of the French Internal Security Code reiterates the principle that a service under the authority of the Prime Minister, separate from the intelligence services, is the only body authorised to carry out processing and operations implemented in the context of algorithmic surveillance.

IMPLEMENTATION CONDITIONS NOW IN LINE WITH EUROPEAN REQUIREMENTS

The application of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights (ECHR):

Applying the principle of the right to respect for private and family life, home and correspondence, protected by Article 8 of the Convention, to electronic surveillance, the ECHR ruled on the conformity with the Convention of mass surveillance measures, which may include the use of algorithms for legal analysis purposes. In its two Grand Chamber rulings of 25 May 2021, the European Court of Human Rights notably found that states party to the Convention may, in order to safeguard their security, resort to mass surveillance of electronic communications, whether the content itself or the associated metadata, provided that the surveillance system in question is clearly defined by law, is necessary, and includes "end-to-end" procedural safeguards (ECHR, 25 May 2021, *Big Brother Watch and others v. United Kingdom*, applications nos. 58170/13, 62322/14 and 24960/15; ECHR, 25 May 2021, *Centrum för Rättvisa v. Sweden*, application no. 35252/08)[39].

The strict legal framework currently surrounding the implementation of algorithmic technology should enable this detection system to be considered as meeting the requirements set by the ECHR.

The question of the application of European Union.

As mentioned in the introduction, intelligence-gathering techniques are, in principle, not governed by European regulations. Nevertheless, such regulations can have an impact on how these techniques are implemented. Thus, in a landmark series of rulings issued in October 2020, the Court of Justice of the European Union (CJEU) ruled that EU law governing the electronic communications and digital data sector prohibits national legislation that imposes, on a preventive basis,

39. For a detailed presentation of these rulings and the requirements set by the European Court of Human Rights (ECHR), see the CNCTR's 6th Annual Activity Report (2021), section 1.2, p. 48.

the general and indiscriminate retention of connection data (CJEU, 6 October 2020, *La Quadrature du Net* and others, cases C-511/18, C-512/18, C-520/18 and C-623/17). However, the availability of such data is necessary for the implementation of certain intelligence-gathering techniques.

This intersection between EU law and national intelligence frameworks could have led to the invalidation of national provisions on the grounds of incompatibility with European rules governing digital activities. However, in a series of decisions dated 21 April 2021, the Council of State upheld the principle of the obligation imposed on electronic communications operators and internet service providers to retain connection data in a generalised and indiscriminate manner, subject to regular confirmation of the persistence of a sufficient threat to national security (CE, Assembly, 21 April 2021, *French Data Network and others*, No. 393099; *La Quadrature du Net and others*, No. 394922 No. 397851; *Association Igwan.net*, No. 397844; *Société Free Mobile*, No. 424717 and *Société Free* No. 424718). Furthermore, the reservations expressed or incompatibilities identified in these decisions concerning the data retention regime and the obligation of prior control of techniques by an independent administrative authority with the power to issue a binding opinion or by a court were lifted by the adoption of the PATR law of 30 July 2021[40].

40. On these points, see the CNCTR's 6th activity report for 2021: appendix 4, CNCTR deliberation no. 4/2021 of 30 April 2021 and appendix 5, decision of the Council of State ruling on the dispute.

2.2. Strict oversight of algorithm deployment

2.2.1. | Thorough ex-ante control

The CNCTR's ex-ante control of algorithms must be particularly rigorous. It is significantly more demanding than for other intelligence-gathering techniques, especially regarding the assessment of the legality and proportionality of initial requests to authorise a new algorithm. Moreover, the commission always issues its opinion through a classified deliberation adopted by the board sitting in plenary session, enabling as detailed an opinion as necessary and allowing for any restrictions deemed appropriate.

This level of control requires the requesting service and the GIC to carry out extensive studies and preparatory work. Such efforts are essential to allow the commission to assess the relevance of the proposed algorithm parameters and the level of intrusiveness of the corresponding processing operations, in addition to reviewing the fundamental justification for using the technique and ensuring that the request complies with legal requirements. The way in which the algorithm is configured determines the operational effectiveness of the detection system, as well as guaranteeing that, while the treatment is not individualised, it is circumscribed and proportionate in its effects.

To ensure a proper balance between these two requirements, the CNCTR's oversight relies on a detailed audit of the proposed algorithm's configuration and operating principles, including, where necessary, an examination of its source code. The commission's review focuses on all elements used by the requesting service to design its algorithm, particularly the behaviours being targeted, as well as the models developed to verify the compliance of

the processing with its description and the reasoning provided by the service, and to assess whether it is sufficiently discriminating. The commission pays particular attention to avoiding situations where it would face a "black box" system.

The CNCTR's ex-ante control of algorithms must be particularly rigorous. It is significantly more demanding than for other intelligence-gathering techniques, especially regarding the assessment of the legality and proportionality of initial requests to authorise a new algorithm. Moreover, the commission always issues its opinion through a classified deliberation adopted by the board sitting in plenary session, enabling as detailed an opinion as necessary and allowing for any restrictions deemed appropriate.

This level of control requires the requesting service and the GIC to carry out extensive studies and preparatory work. Such efforts are essential to allow the commission to assess the relevance of the proposed algorithm parameters and the level of intrusiveness of the corresponding processing operations, in addition to reviewing the fundamental justification for using the technique and ensuring that the request complies with legal requirements. The way in which the algorithm is configured determines the operational effectiveness of the detection system, as well as guaranteeing that, while the treatment is not individualised, it is circumscribed and proportionate in its effects.

To ensure a proper balance between these two requirements, the CNCTR's oversight relies on a detailed audit of the proposed algorithm's configuration and operating principles, including, where necessary, an examination of its source code. The commission's review focuses on all elements used by the requesting service to design its algorithm, particularly the behaviours being targeted, as well as the models developed to verify the compliance of the processing with its description and the reasoning provided by the service, and to assess whether it is sufficiently discriminating. The commission pays particular attention to avoiding situations where it would face a "black box" system.

The in-depth reviews and verifications carried out, combined with the dialogue established throughout the development and modification phases of each algorithm with the GIC and the requesting service, enable a collaborative approach to developing this technique, ensuring its acceptability. The five algorithms currently in use were all developed following such an approach, which closely involved the CNCTR, the GIC and the requesting services in the development of the system[41].

Although the checks carried out on renewal requests gradually become less sensitive once the algorithm is stable, they are nevertheless carried out with greater vigilance to ensure compliance with the legal framework and the proportionality of the technique. This review also takes into account the operational results presented by the GIC and the service concerned. Furthermore, as a sign of the importance attached by the CNCTR to the control of requests for renewal of algorithms, their examination is always carried out by its board sitting in plenary session, although this is not required by law.

The demanding control carried out by the CNCTR can be illustrated by the process followed for the deployment of the first algorithm in 2017[42].

After extensive discussions on the architecture to be adopted for the algorithms, the CNCTR received a request for the initial implementation of an automated processing system based on Article L. 851-3 of the French Internal Security Code. It carried out a preliminary audit, both on-site and off-site, to check that the algorithm, and in particular its source code, complied with the description given in the application. By means of a classified deliberation adopted in plenary session on 26 July 2017, it concluded that the processing presented, by its technical characteristics and function, corresponded to the legal definition of

41. See p. 42 of this report.

42. This process is described in detail in the 2nd annual report 2017 of the CNCTR, available on its website.

the algorithm and confirmed its conformity with the description submitted by the service. It also considered that the use of this processing would not result in a breach of privacy disproportionate to the terrorist threat to be prevented. Nevertheless, it issued an unfavourable opinion on the implementation of the processing operation, after noting that it was not surrounded by sufficient safeguards.

Following a new request concerning the same algorithm, the CNCTR, after noting the additional safeguards proposed, issued on 5 October 2017 a favourable opinion for an initial implementation of this processing for a period of two months, in accordance with Article L. 851-3 of the French Internal Security Code. After receiving a request for renewal at the end of this period, the commission issued an opinion in favour of the renewal, provided that it was again limited to a period of two months. In the light of the initial results, it was felt that the automated processing system should be re-examined in the near future to ensure the relevance and reliability of its technical characteristics. This advice was followed by the Prime Minister.

As for the control carried out on requests for lifting anonymity, this proves to be all the simpler and easier when the algorithmic system has been properly configured and verified. It has enabled the CNCTR to detect any instability in the processing, which could manifest, for example, in an abnormal number of alerts compared with the system's development work, and to recommend their immediate suspension. As evidence of the work done on this point, the impact assessment of 11 May 2021 mentioned above[43] noted, for example, that the configuration of the three algorithms in operation in 2020 had made it possible to limit the frequency of alerts while maintaining a useful detection threshold.

43. See note 38.

2.2.2.| A diversified ex-post control

The most common ex-post control involves the CNCTR assessing the results of the algorithms presented by the services when they apply for renewal or modification, in which case the law has taken care to give the CNCTR the means to carry out effective control by stipulating in particular that it must be "*informed of any changes made to the processing and parameters*" of automated processing and have "*permanent, complete and direct access to such processing operations and to the information and data collected*"[44].

In addition to these regular controls, the Prime Minister may also, on a more ad hoc basis, draw up general reports on algorithmic surveillance, which are the subject of classified evaluation reports enabling the recipients, the CNCTR and the DPR, to assess the usefulness of the technique and the extent to which it undermines the protection of privacy and personal data, or public reports intended, in particular, for national representatives.

In addition to these controls based on documentation, further checks are also carried out, for example following technical or organisational changes, notably through audits of algorithm source codes, inspections of the practical arrangements for centralisation by the GIC, and examination of the information and data collected *via* automated processing. In this regard, the commission ensures compliance not only with legal requirements, but also with the recommendations made during the development of the technical architecture of the algorithms.

The use of algorithms by public intelligence policy in France does not make this technique a form of mass surveillance, since it does not allow intelligence services to know the occupations of a multitude of precisely identified or identifiable persons. On the contrary,

44. Article L. 851-3 of the French Internal Security Code.

its purpose is to anonymously highlight clues that can be used to lift anonymity, under strict control.

The law has permitted this use in order to improve the intelligence services' ability to detect serious threats; it has ensured the necessary balance of the system by giving the CNCTR end-to-end control. The commission exercises this power to the full.

It is for the legislature to assess whether the general interest justifies the use of algorithmic techniques for one of the purposes strictly defined by the French Internal Security Code. Initially reserved for the fight against terrorism, this use has been extended to the fight against foreign interference and will be extended in the future to the fight against drug trafficking, which appears to have become a threat to the normal functioning of our institutions, as noted by the commission in its 2023 activity report.

For its part, the CNCTR will continue, in conjunction with the intelligence services and the Inter-Ministerial Control Group, to monitor and ensure the balance that it is responsible for safeguarding.

Appendices

1. Changes in the composition of the college during 2024

The composition of the board of the CNCTR changed significantly in 2024.

On 2 October 2024, the terms of office of Ms Françoise Sichler-Ghestin, Honorary Member of the Council of State, and Mr Gérard Poirotte, Honorary Councillor at the court of Cassation, came to an end. They were replaced by Ms Magali Ingall-Montagnier, counsellor at the Court of Cassation, and Mr Didier Chauvaux, Honorary Member of the Council of State. Furthermore, the dissolution of the National Assembly on 9 June 2024 led to the end of the terms of office of Ms Michèle Tabarot and Mr Yannick Chenevard. They were replaced by Ms Émilie Bonnivard, Member of Parliament for Savoie, and Mr Christophe Naegelen, Member of Parliament for Vosges, appointed on 6 November 2024.

At the end of 2024, the board of the CNCTR was made up of the following **nine members**:

- **Mr Serge Lasvignes**, Honorary Member of the Council of State, Chairman;
- **Ms Chantal Deseyne**, Senator for Eure-et-Loir;
- **Mr Jérôme Darras**, Senator for Pas-de-Calais;
- **Ms Émilie Bonnivard**, Member of Parliament for Savoie;
- **Mr Christophe Naegelen**, Member of Parliament for Vosges;
- **Mr Didier Chauvaux**, Honorary Member of the Council of State;
- **Ms Solange Moracchini**, Honorary Advocate General at the Court of Cassation;
- **Ms Magali Ingall-Montagnier**, counsellor at the Court of Cassation;
- **Mr Philippe Distler**, qualified expert in electronic communications.

Following the resignation of Chairman Lasvignes in January 2025, Ms Solange Moracchini was appointed interim chairwoman[1], then, by decree of 28 March 2025[2], Mr Vincent Mazauric was appointed Chairman of the commission.

The procedures for appointing or nominating members are set out in Article L. 831-1 of the French Internal Security Code and, where applicable, in the provisions of law no. 2017-55 of 20 January 2017 on the general status of independent administrative authorities and independent public authorities. With the exception of members of

1. See the decree of 31 January 2025 of the President of the Republic appointing Ms Moracchini, member of the college, as interim chair from 1 February 2025.
2. See the decree of 28 March 2025 of the President of the Republic appointing the chairman of the National Oversight Commission for Intelligence-Gathering Techniques, published in the Official Journal on 29 March.

parliament, their term of office is six years and is not renewable. Half of the members of the Council of State and the Court of Cassation are renewed every three years. In addition, except for the qualified expert, the law provides that the appointment or nomination procedures for commission members must ensure gender parity.

Under Article 5 of the Act of 20 January 2017 on the general status of independent administrative authorities and independent public authorities, a member appointed to replace another member whose term ended early is appointed for the remaining duration of that term. If the remaining duration is less than two years, this term is not counted for the purpose of applying the non-renewal rule set out in Article L. 831-1 of the French Internal Security Code.

2. The resources of the CNCTR in 2024

2.1. Human resources

Since the end of November 2023, four of the nine members of the commission have been serving full-time. These are the CNCTR chairman, the two members of the Court of Cassation and the qualified expert.

The provisions of the French Internal Security Code require the CNCTR to issue its opinions on requests for the use of intelligence-gathering techniques that do not require examination by the full panel within 24 hours. These opinions may only be issued by members who are magistrates. Where the request falls under the responsibility of the board sitting in plenary session or the board sitting in restricted session, or where it is referred to such a formation, the time limit is extended to seventy-two hours. Consequently, these board committees meet, except in exceptional circumstances, three times a week, on Mondays, Wednesdays and Fridays. Each month, the CNCTR holds a formal meeting of all its members in plenary session. These meetings examine the most important draft resolutions and include time devoted to the work of the committee, both in terms of substantive issues and statistical data.

In addition to these collegial training sessions, frequent meetings, presentations and hearings are organised with the intelligence services on the commission's premises, in order to enlighten the board on technical or legal issues.

Full-time members also take part in service audits.

At the end of 2024, the CNCTR was carrying out its mission with a team of 22 agents, led by a general secretary and comprising an advisor

to the Chairman, 14 mission officers and four support staff: a budget and human resources manager responsible for overseeing the secretariat, two executive assistants and a multi-skilled officer who also serves as deputy security officer. The CNCTR has also strengthened its information systems department with the recruitment of a network administrator.

The CNCTR's mission officers are category A+ agents or equivalent, whose main role is to investigate requests for the use of intelligence-gathering techniques and to carry out ex-post controls, under the supervision of a member of the commission.

They are either seconded or assigned public officials: judicial and administrative magistrates, police commissioners, gendarmerie officers, chief weapons engineers, customs inspectors, or contract staff, particularly engineers.

The secretariat is staffed by two permanent civil servants and two contract staff.

The team has equal representation: 11 men and 11 women. The average age of our staff is 39 years.

In accordance with the provisions of article L. 832-5 of the French Internal Security Code, all Commission staff are authorised to maintain the national defence secrecy.

2.2. The budget

The funds allocated by Parliament to the CNCTR in the Finance Act are part of the "Government Action Directorate" budget, which covers the funds and expenditure of the Prime Minister's services and independent authorities. This mission consists of two programmes: programme 129 "Coordination of Government Work" and programme 308 "Protection of rights and freedoms". Programme 308 groups together the appropriations of ten

independent authorities carrying out their missions in the field of the protection of human rights and public and individual freedoms, including the CNCTR[3].

The Finance Act for 2024[4]allocated just over €3 million to the CNCTR for personnel expenditure (Title II) and just over €480,000 for operating expenditure, representing approximately 2.5% of the budget for programme 308. However, the operating appropriations initially planned were significantly affected by the cancellations of appropriations at the beginning of 2024[5] and reduced to just under €450,000 (a reduction of more than 7%).

While the appropriations allocated in 2024 made it possible, in particular, to set up an IT systems unit staffed by dedicated agents, with the aim, among other things, of securing the commission's internal IT system, the constant increase in its volume of activity and the strengthening of its missions in line with legislative and regulatory changes in the field of intelligence are putting pressure on its staff and resources.

While the Finance Act for 2025[6]does not provide for any new posts and its operating appropriations have been reduced once again, **the CNCTR highlights the growing tension between the changing nature of its tasks** (increase in the number of requests, increase in the volume of data collected, greater complexity of controls, etc.) **and the resources at its disposal**. This tension also affects management and support functions, where staffing levels are currently insufficient to ensure that the commission can function in a fully satisfactory manner.

3. In addition to the CNCTR, programme 308 also includes funding allocated to the Defender of Rights, the National Commission for Information Technology and Civil Liberties (CNIL), the General Inspector of Places of Deprivation of Liberty (CGLPL), the Commission for Access to Administrative Documents (CADA), the Commission for the Protection of National Defence Secrecy (CSDN), the High Authority for Transparency in Public Life (HATVP), the Regulatory Authority for Audiovisual and Digital Communication (ARCOM), the National Consultative Ethics Committee for Life Sciences and Health (CCNE) and the National Consultative Commission on Human Rights (CNCDH).

4. See Finance Act 2023-1322 of 29 December 2023 for 2024.

5. See Decree no. 2024-124 of 21 February 2024 cancelling appropriations.

6. See Finance Act 2025-127 of 14 February 2025 for 2025.

3. External relations

During 2024, the commission continued its constructive dialogue with its institutional partners, the academic world and its foreign counterparts. For the first time since its creation, it organised two symposiums open to the public, thereby providing wider access to its missions and analyses (3.1). Furthermore, as in previous years, the commission made several appearances before Parliament (3.2) and provided training to various public entities (3.3). These numerous exchanges and interactions, both at the national (3.4) and international (3.5) levels, enable the commission to present its views on the legal framework for intelligence. They promote awareness of this legal framework, improve practices and enrich mutual understanding.

3.1. Opening up the commission's missions and analyses to the general public through the organisation of two symposiums

An international conference co-organised with the journal *Etudes françaises de renseignement et du cyber* (EFRC).

On **15 October 2024**, the CNCTR, in collaboration with the journal *Etudes françaises de renseignement et du cyber* (PUF), co-organised **a conference on the challenges of controlling intelligence services and, more specifically, on dialogue between oversight bodies**.

Organised around three thematic round tables, it brought together public officials from the intelligence community, magistrates, members of oversight bodies from other European states, academics and experts in surveillance techniques. The discussions provided an opportunity to debate data and technology control

methods, examine different models of intelligence service control implemented in Europe, and question the coexistence in France of multiple intelligence service oversight bodies, including Parliament, the Council of State, the *Cour des comptes*, independent administrative authorities or internal inspection or oversight bodies.

For the first time since the commission was created, this event was open to the general public. It brought together nearly 350 participants[7].

A symposium co-organised with the National Commission for Information Technology and Civil Liberties (CNIL) - "Surveillance in all its forms. What ethical framework to protect our freedoms?".

For several years, the CNIL has been organising public debates on new digital issues, bringing together expertise from the field and the scientific community: this is the aim of the "Air" events[8]. In 2024, the CNCTR was invited by the CNIL to co-organise this event on the theme of **surveillance in all its forms and its ethical challenges**.

In order to offer a forward-looking reflection on surveillance, this symposium, held on **19 November 2024**, brought together public officials from the intelligence community, political scientists, sociologists, experts in surveillance techniques, institutional representatives and civil liberties associations, who were able to exchange views during two round tables devoted to the challenges of peer and interpersonal surveillance and the ethics of intelligence services[9].

This hybrid event (videoconference and in-person) brought together nearly 1,700 people to discuss these issues, thereby raising awareness of surveillance issues, particularly those involving intelligence services, for the benefit of all citizens.

7. See the proceedings of the symposium published in issue no. 4 of the EFRC journal or on the Cairn website https://shs.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2024-2?lang=fr

8. For "futures, innovations, revolutions".

9. In March 2025, the CNIL and the CNCTR published a series of interviews and testimonials covering the various topics discussed at the event. See the CNCTR and CNIL websites: https://www.cnctr.fr/actes-colloque-air2024#le-cahier-air2024 and https://www.cnil.fr/fr/cahier-air2024.

The CNCTR also continued its efforts to provide the general public with information, as detailed as possible given the requirements of national defence secrecy, on its mission and the exercise of its control activities.

Following the overhaul of its website[10] in 2023, the commission expanded the resources available on the site, including activity reports, thematic fact sheets and translations into English.

3.2. An ongoing dialogue with Parliament

During 2024, the chairman of the CNCTR was heard on several occasions by Parliament. Beyond the option provided for in Article L. 833-11 of the French Internal Security Code, which allows the president of the National Assembly, the president of the Senate, and the Parliamentary Intelligence Committee to request opinions from the commission, these hearings reflect the ongoing dialogue maintained with Parliament year after year.

Chairman Lasvignes was heard twice by the Senate. In April, at the initiative of Ms Agnès Canayer, rapporteur for the **bill aimed at preventing foreign interference in France**[11] for the Law Commission, he was questioned in particular on the extension of the technique known as the algorithm for the purposes mentioned in points 1 and 2 of Article L. 811-3 of the French Internal Security Code (see the study devoted to this technique, p. 141). In June, he presented the CNCTR's activity report for 2023 to the Law and Defence Commissions.

He was heard twice by the National Assembly. In March 2024, Mr Sacha Houlié, Chairman of the Law Commission, author and rapporteur of the **bill aimed at preventing foreign interference**

10. https://www.cnctr.fr/

11. See the legislative file on the Senate website: Foreign interference in France - Senate.

in France[12], invited him to speak on the appropriateness and legal issues of extending the use of algorithms to new purposes. In September, he was able to meet with Ms Yaël Braun-Pivet, President of the National Assembly, to present the CNCTR's activity report for 2023 and the areas of vigilance highlighted by the commission in the report.

In addition, the Parliamentary Intelligence Committee, which includes elected representatives from both the National Assembly and the Senate, heard him twice in 2024. In May, he was heard in particular on the CNCTR's activity report for 2023, on the extension of algorithm technology in the context of the draft law aimed at preventing foreign interference in France, and on the prospects and challenges identified by the commission for the coming years. In November, he was able to discuss with the delegation the activities of the intelligence services in the context of the organisation of the Olympic and Paralympic Games, as well as possible developments in the legal framework.

3.3. Training courses to which the commission has contributed

In 2024, the commission once again contributed to the training of intelligence service agents and senior officials from their supervisory ministries in order to develop their knowledge of the legal framework applicable to intelligence-gathering techniques. The commission thus made nearly a dozen appearances in 2024 before students at the **Intelligence Academy**. In addition, it contributed to three continuing education sessions provided by the **National School for the Judiciary**.

12. See the legislative file on the National Assembly website: Preventing foreign interference in France - Legislative files - 16th → 16th legislature - National Assembly.

3.4. The other institutional counterparts of the commission

Chairman Lasvignes was heard twice by the Council of State: once in January 2024, as part of its annual study on sovereignty[13], and a second time to present the commission's activity report for 2023 to the interior section.

3.5. The international relations of the commission

During 2024, the CNCTR maintained dialogue with its foreign counterparts at bilateral and multilateral meetings.

On 13 June 2024, a delegation from the commission took part in the **International Conference on Privacy Protection** in Venice, which brings together national supervisory authorities from many countries and academics every year.

Discussions focused in particular on the different procedures in France and other countries, such as the United States and Canada, for handling complaints or appeals from individuals wishing to verify that no intelligence-gathering techniques are being or have been used unlawfully against them.

Furthermore, during the symposium held on 15 October 2024[14], a round table was devoted to an exchange between representatives of the supervisory bodies of the intelligence services of Germany[15], Denmark[16] and the United Kingdom[17].

13. See: https://conseil-etat.fr/publications-colloques/etudes/etude-annuelle-sur-la-souverainete.
14. See above.
15. G 10 - Kommission.
16. Danish Intelligence Oversight board (TET).
17. Investigatory Powers Commissioner's Office (IPCO).

4. Glossary

A

- **Administrative policing**

  Measures taken by an administrative authority to prevent, in particular, disturbances to public order or infringements on civil peace. Administrative policing is distinct from judicial policing, which aims to prosecute the commission of such offences.

- **Algorithm**

  Automated processing of connection data, the use of which, provided for under Article L. 851-3 of the French Internal Security Code, may only be authorised for the sole purpose of preventing terrorism.

  The algorithm is designed to detect, within connection data transiting over the networks of electronic communications operators, including URLs, indicators that may reveal the preparation of a terrorist act, such as a pattern of connections that reflects behaviour indicative of a threat.

C

- **Computer data collection**

  Physical or remote access to computer data stored in an information system, or to data flows received, transmitted, or processed by such a system, including peripherals such as a keyboard, computer screen, or microphone.

  The implementation of this technique, provided for under Article L. 853-2 of the French Internal Security Code, may involve agents entering private premises, including residential dwellings.

The procedure for obtaining authorisation to use this technique, identical to that which applies to the recording of words or images in a private location, requires a deliberation by the CNCTR, which must ensure that the infringement of privacy of the person concerned is strictly proportionate to the seriousness of the threat or stakes involved, and that the use of this technique is the only means of obtaining the intelligence sought.

- **Content**

  Access to the content of a communication allows one to know the entirety of a correspondence: it is the letter inside an envelope or the message within an email.

  This notion is distinct from the container, such as the envelope in which the letter is contained, which only reveals the identity and address of the sender and recipient, without it being possible to deduce the content of their correspondence: it is the identifier, telephone number or e-mail address of a person and their correspondent.

E

- **Extraction**

  The retrieval, for analytical purposes, of part of the raw data collected during the implementation of an intelligence-gathering technique, such as images or words.

- **Ex-ante control**

  The CNCTR verifies the legality of all requests to implement intelligence-gathering techniques on national territory, before they are submitted for authorisation by the Prime Minister.

Ex-post control

To ensure comprehensive and effective oversight of the activities of the intelligence services, the legislator has assigned a specialised body, the CNCTR, powers to carry out verifications covering all stages of the procedure for implementing intelligence-gathering techniques. In addition to the ex-ante examination of requests from the services seeking to use such techniques, the commission also monitors the implementation of authorised techniques: this is ex-post control.

F

Fundamental interests of the Nation

A concept defined in Article 410-1 of the French Criminal Code, the fundamental interests of the Nation "*are understood to mean (…) its independence, the integrity of its territory, its security, the republican form of its institutions, the means of its defence and diplomacy, the safeguarding of its population both in France and abroad, the balance of its natural environment, and the essential elements of its scientific and economic potential and its cultural heritage*."

The legislator has drawn on this definition to frame the activities of the intelligence services: the law thus makes the use of intelligence-gathering techniques conditional on the defence or promotion of the fundamental interests of the Nation, which are exhaustively listed in Article L. 811-3 of the French Internal Security Code. The fundamental interests of the Nation that may justify the implementation of intelligence-gathering techniques are:

- National independence, territorial integrity and national defence;
- The major interests of foreign policy, the execution of France's European and international commitments and the prevention of any form of foreign interference;

- The economic, industrial and scientific interests of the France;
- The prevention of terrorism;
- The prevention of damage to the republican form of the institutions, the prevention of actions aimed at maintaining or rebuilding dissolved groups and the prevention of collective violence likely to seriously harm public peace;
- The prevention of organised crime and delinquency;
- The prevention of the proliferation of weapons of mass destruction.

G

- **Geolocation device**

  This intelligence-gathering technique, provided for under Article L. 851-5 of the French Internal Security Code, consists of placing a "tracking device" in contact with a target in order to monitor their movements, those of their vehicle, or an object belonging to them.

I

- ***IMSI catcher***

  Proximity capture device that functions like a fake relay antenna. Its use makes it possible to intercept connection data or correspondences exchanged by mobile terminals that have connected to it.

- **Independent administrative authorities**

  State administrations, but with a status that guarantees the independence of their members from the Government, the independent administrative authorities are entrusted by

the legislature with specialised tasks that it cannot itself carry out directly. These missions may involve protecting rights or regulating economic activities. In the field of intelligence, the CNCTR has been entrusted by law with the task of overseeing the legality of intelligence-gathering techniques used by the intelligence services. The status and list of independent administrative authorities were established by law no. 2017-55 of 20 January 2017 on the general status of independent administrative authorities and independent public authorities.

Inter-Ministerial Control Group

Reporting to the Prime Minister, the Inter-ministerial Control Group (GIC) is responsible for centralising all requests for the implementation of intelligence-gathering techniques, the authorisations for their implementation issued by the head of government, the execution of certain authorisations and the intelligence gathered pursuant to these authorisations.

The GIC, which is not an intelligence service, has exclusive responsibility for liaising with electronic communications operators for the implementation of certain intelligence-gathering techniques, such as security intercepts. It executes the authorisations issued by the Prime Minister on behalf of the services and provides them with the results of implementation.

Intelligence

A preventive action falling within the scope of administrative policing, which only the intelligence services may carry out. It consists of searching for, collecting, and analysing information relating to the fundamental interests of the Nation, with the aim of defending or promoting them in the face of threats and risks likely to affect them.

The activities of the intelligence services may require the use of techniques that infringe upon civil liberties, including the right to privacy.

Intelligence service

A State administration legally authorised to use intelligence-gathering techniques.

Intelligence-gathering technique

A means of gathering intelligence, the use of which, in the absence of authorisation given within the framework of the law, would constitute a criminal offence.

International electronic communication

Electronic communication sent or received abroad.

The communications concerned can only be intercepted by decision of the Prime Minister, who then designates the networks concerned. Intercepted communications may then be used for surveillance purposes for all purposes provided for by law, if the Prime Minister, after consulting the CNCTR, authorises it.

Internet connection data

Information that enables the routing of an electronic communication. This is comparable to the information that appears on the envelope of a letter to ensure it reaches its recipient, such as the name and address of the sender and recipient.

It is defined in Article L. 851-1 of the French Internal Security Code as "*information or documents processed or stored*" by "*networks*" or "*electronic communications services*" of electronic communications operators, hosting providers, and internet service providers, "*including technical data relating to the identification of subscription or connection numbers to electronic communications services, the listing of all subscription or connection numbers linked to a specific person, the location of the terminal equipment used, as well as subscriber communications involving the list of incoming and outgoing numbers, the duration, and the date of communications*."

The collection of this data constitutes a lesser infringement on the privacy of the persons concerned than accessing their correspondence, meaning the contents inside the envelope. However, the volume of electronic communications is such that access to connection data can reveal or allow deduction of a significant amount of information about an individual's private life, such as daily routines, places of residence, or movements.

P

- **Parliamentary Intelligence Committee**

  A parliamentary body common to both the National Assembly and the Senate, tasked with overseeing government action in the field of intelligence and evaluating public policy in this area. It is composed of eight members: four deputies and four senators.

- **Plenary formation**

  Formation of the CNCTR board comprising all its members, namely the four parliamentary members, the four members from the judiciary, and the qualified expert in the field of electronic communications.

  This is the Commission's most formal formation, which meets at least once a month. A meeting of the plenary formation is mandatory when the CNCTR is asked to examine a request to implement an intelligence-gathering technique targeting a person holding a parliamentary mandate or practising as a lawyer, journalist, or magistrate.

- **Principle of proportionality**

  Principle whereby there must be a balance between the means employed and the intended objective.

In applying this principle, the CNCTR assesses the legality of the implementation of intelligence-gathering techniques: it ensures that the infringement of privacy resulting from the use of a technique is proportionate to the seriousness of the threat it seeks to prevent.

For the most intrusive techniques involving entry into a private premises, this requirement of proportionality also implies a subsidiarity check by the commission: as provided by law, it must verify, in accordance with this principle, that the intelligence sought could not be effectively obtained by other lawful means that are less intrusive to privacy.

- **Purpose**

  The objective pursued by an intelligence service.

  Article L. 811-3 of the French Internal Security Code lists a limited number of entities that may legally authorise the intelligence services to use these techniques: their objective is the defence and promotion of the fundamental interests of the Nation, which the law defines in seven distinct and exhaustive categories.

Q

- **Quorum**

  Any new or serious question is referred to the restricted session or the plenary session. The restricted session and the plenary session may only validly deliberate if, respectively, at least three and four members are present. Decisions are taken by a majority of the members present.

  In the event of a tie, the chairman has the casting vote (Article L. 832-3 of the French Internal Security Code).

Quota system

Principle according to which the number of simultaneous authorisations to use a technique may not exceed a quota set by the Prime Minister, after consulting the CNCTR. The aim of limiting the maximum number of surveillance operations is to encourage services to use techniques only when necessary and to terminate authorisations that are no longer required before applying for new ones. In particular, it applies to techniques such as the collection of connection data in real time and security interceptions, the implementation of which may concern not only the individuals placed under primary surveillance but also their associates. The quota system thus makes it possible to limit to what is strictly necessary the number of persons likely to be targeted.

R

Real-time geolocation

Device for locating a person on a map in real time.

Its implementation, as provided for in Article L. 851-4 of the French Internal Security Code, consists of locating a person's terminal communications equipment, such as a mobile phone. It requires the involvement of an electronic communications operator, who queries their network and transmits the data obtained to the Inter-Ministerial Control Group, a service under the authority of the Prime Minister.

Restricted formation

Formation of the CNCTR board comprising the four members exercising judicial functions and the qualified expert in the field of electronic communications.

Requests to implement intelligence-gathering techniques involving entry into a dwelling or computer data collection in a private location require deliberation by the board sitting in restricted session.

Recording of words

Sound recording of certain places or recording of words spoken in a private or confidential capacity, under the terms of article L. 853-1 of the French Internal Security Code, which provides for the authorisation to use this technique.

The devices used for such capture, such as a microphone, may be installed in a private place: the procedure for obtaining authorisation to use this technique, identical to that which applies to the recording of images in a private place or the collection of computer data, requires a collegial decision by the CNCTR, which must then ensure that the infringement of privacy of the person concerned is strictly proportionate to the importance of the threat or the issues involved and that the use of this technique represents the only means of obtaining the information sought.

Recording of images

Taking of photographs or recording of video footage in a private place.

The intelligence services may be authorised to use this intelligence-gathering technique under Article L. 853-1 of the French Internal Security Code, by entering a private location.

To be authorised to use this technique, a service must convince the CNCTR not only that the infringement of privacy resulting from its use is strictly proportionate to the importance of the threat or the issues involved, but also that this technique is the only way for it to obtain the information it is seeking.

S

- **Specialised intelligence services – "first circle" services**

  There are six specialised intelligence services (DGSE, DGSI, DNRED, DRM, DRSD, and Tracfin) that have been assigned by the legislator the tasks of searching for, collecting, exploiting, and providing the Government with "*intelligence relating to geopolitical and strategic issues as well as threats and risks likely to affect national life*." The law specifies that "*they contribute to understanding and anticipating these issues, as well as to preventing and countering such risks and threats*."

  In this context, these services, with the exception of the Directorate of Military Intelligence (DRM) and Tracfin, are authorised to use the full range of intelligence-gathering techniques provided for by law, provided that their use falls within at least one of the seven purposes that may legally justify such recourse.

- **Security interception**

  Security interception, or administrative interception of correspondences, allows the listening of a person's telephone conversations or the reading of their written correspondences, meaning access to the content of their communications. The authorisation to use this technique also permits access to the connection data relating to these communications.

- **"Second circle" services**

  Commonly referred to as "second circle" services, in contrast to the "first circle" made up of the specialised intelligence services, these services either carry out intelligence activities as only part of their overall missions or belong to an administration whose responsibilities go beyond intelligence alone. They may only use **certain intelligence-gathering techniques** provided for by law and only for a limited number of purposes.

They include departments within the **Directorate General of the National Police**, the **Directorate General of the National Gendarmerie**, the **Paris Police Prefecture, and the Prison Administration**.

Most of these services, around twenty, do not carry out intelligence as their sole mission. This includes, for example, **judicial police services**, such as the National Directorate of the Judicial Police, or certain **territorial services** with general duties, such as the National Gendarmerie's regional investigation sections.

Four of them, on the other hand, are entrusted with an exclusive intelligence mission: the **National Directorate of Territorial Intelligence within the Directorate General of the National Police**, the **Intelligence Directorate of the Paris Police Prefecture**, the Sub-Directorate of Operational Anticipation within the Directorate General of the National Gendarmerie and the **National Prison Intelligence Service** within the Directorate of Prison Administration.

T

Transcription

The action of writing down, for analytical purposes, what the implementation of a technique has made it possible to see or hear.

Traceability sheets

Under the terms of Article L. 822-1 of the French Internal Security Code, a statement of implementation of each intelligence-gathering technique, mentioning "*the start and end dates of implementation as well as the nature of the information collected*", shall be established. This record, more commonly referred to as a "*traceability sheet*", "*must be made available to the commission, which shall have permanent, full and direct access to it, regardless of its degree of completion.*"

U

URL

A URL, or ***Uniform Resource Locator***, is an alphanumeric string that identifies the address of content on the Internet, such as a webpage.

This type of connection data may relate to the content of information consulted by Internet users.

Such data therefore falls under both connection data, which is necessary for the routing of a communication, and content data, as it provides indications regarding the content of the information consulted.

5. Provisions of the French Criminal Code relating to “R. 226” regulations

Legislative part

BOOK II: Crimes and offences against the person

Title II: Offences against the human person

CHAPTER VI OFFENCES AGAINST THE PERSON

Section 1 Infringements of privacy

Article 226-1 of the French Criminal Code

Any person who, by any means, deliberately infringes on another person's privacy is liable to one year's imprisonment and a fine of €45,000:

1. By capturing, recording, or transmitting, without the consent of the speaker, words spoken privately or confidentially;

2. By taking, recording or transmitting, without the consent of the person concerned, the image of a person in a private place.

3. By capturing, recording, or transmitting, by any means, the real-time or delayed location of a person without their consent.

Where the acts referred to in 1.and 2.of this article have been carried out openly and visibly in front of the persons concerned, and they do not object when able to do so, their consent is presumed.

Where the acts referred to in this article have been performed on a minor, consent must be given by the holders of parental authority, in accordance with Article 372-1 of the French Civil Code.

If the offence is committed by the victim's spouse or partner, or civil union partner, the penalties are increased to two years' imprisonment and a fine of €60,000.

If the offence is committed against a person holding public authority, carrying out a public service mission, holding or standing for elected office, or a member of their family, the penalties also increase to two years' imprisonment and a €60,000 fine.

Article 226-3 of the French Criminal Code

The following acts are punishable by five years' imprisonment and a fine of €300,000:

1. The manufacture, import, possession, display, offer, rental, or sale of equipment or technical devices likely to enable the commission of the offence under the second paragraph of Article 226-15, or designed for the remote detection of conversations that allow the offence under Article 226-1, or intended for the collection of computer data as provided for under Articles 706-102-1 of the French Code of Criminal Procedure and Article L. 853-2 of the French Internal Security Code, and listed under conditions defined by decree of the Council of State, when these acts are carried out, including through negligence, without the ministerial authorisation required by the same decree, or without complying with the conditions set by that authorisation;

2. Advertising such equipment or devices if it constitutes an incitement to commit the offences under Article 226-1 or the second paragraph of Article 226-15, or advertising devices intended for the collection of computer data under Articles 706-102-1 of the French Code of Criminal Procedure and L. 853-2 of the French Internal Security Code, if the advertising constitutes an incitement to misuse such equipment.

This article does not apply to possession or acquisition of such equipment by the operators mentioned in Article L. 1332-1 of the French Defence Code, designated as such due to their operation of a public electronic communications network, provided they hold the necessary authorisation from the Prime Minister under Section 7 of Chapter II, Title I, Book II of the Postal and Electronic Communications Code.

Section 4 Infringements of secrecy

Paragraph 2 Infringements of the secrecy of correspondence

Article 226-15 of the French Criminal Code

The act, committed in bad faith, of opening, destroying, delaying, or diverting correspondence, whether or not it has reached its intended recipient, when addressed to third parties, or of fraudulently becoming aware of its contents, is punishable by one year of imprisonment and a fine of €45,000.

The same penalties apply to the act, committed in bad faith, of intercepting, diverting, using, or disclosing correspondence sent, transmitted, or received by electronic means, or of installing devices designed to enable such interceptions.

If these acts are committed by the victim's spouse or partner, or civil union partner, the penalty is increased to two years of imprisonment and a fine of €60,000.

Regulatory Part

BOOK II: Crimes and offences against the person Title

II: Offences against the human person CHAPTER VI

OFFENCES AGAINST THE PERSON

Section 1 Infringements of privacy

Article R. 226-1 of the French Criminal Code

The list of devices and technical equipment referred to in Article 226-3 is established by order of the Prime Minister.

Notwithstanding the provisions of Article 1 of Decree no. 97-34 of 15 January 1997 relating on the decentralisation of individual administrative decisions, the authorisations provided for in Articles R. 226-3 and R. 226-7 are issued by the director general of the National Cybersecurity Agency (ANSSI).

Article R. 226-2 of the French Criminal Code

A consultative commission is established under the authority of the Prime Minister, composed as follows:

1. The director general of the National Cybersecurity Agency (ANSSI), or their representative, acting as chair;
2. A representative of the Minister of Justice;
3. A representative of the Minister of the Interior;
4. A representative of the Minister of Defence;
5. A representative of the Minister responsible for customs;

6. A representative of the Minister responsible for industry;

7. A representative of the Minister responsible for telecommunications;

8. A representative of the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR);

9. A representative of the director general of the National Frequency Agency;

10. Two people chosen for their expertise, appointed by the Prime Minister.

The commission may consult, as experts, any qualified person.

It is consulted for its opinion on draft orders issued under Articles R. 226-1 and R. 226-10. It may make proposals for amendments to these orders.

The commission is also consulted on requests for authorisation submitted under Articles R. 226-3 and R. 226-7.

The secretariat of the commission is provided by the National Cybersecurity Agency (ANSSI).

Article R. 226-3 of the French Criminal Code

The manufacture, importation, exhibition, offer, rental, or sale of any device or technical equipment listed under Article R. 226-1 is subject to authorisation, following the opinion of the commission referred to in Article R. 226-2.

Article R. 226-4 of the French Criminal Code

Applications for authorisation must be submitted to the director general of the National Cybersecurity Agency (ANSSI). The application must include, for each type of device or technical equipment:

1. The name and address of the applicant, if a natural person, or its name and registered office, if a legal entity;

2. The operation(s) referred to in Article R. 226-3 for which authorisation is sought and, where applicable, a description of the target markets;

3. The purpose and technical characteristics of the type of equipment or technical device, accompanied by technical documentation;

4. The intended place of manufacture of the appliance or technical device or for other operations mentioned in Article R. 226-3;

5. A commitment to comply with the necessary inspections to verify the accuracy of the information provided in the authorisation application.

Article R. 226-5 of the French Criminal Code

The authorisation referred to in Article R. 226-3 is issued for a maximum period of six years.

It may specify the conditions for carrying out the authorised operation and the number of devices or technical equipment concerned.

It is automatically granted to State departments designated by order of the Prime Minister for the manufacture of such devices or technical equipment.

Article R. 226-6 of the French Criminal Code

Each device or piece of technical equipment manufactured, imported, exhibited, offered, rented, or sold must bear the type reference corresponding to the authorisation application and an individual identification number.

Article R. 226-7 of the French Criminal Code

The acquisition or possession of any device or technical equipment listed under Article R. 226-1 is subject to authorisation, following the opinion of the commission referred to in Article R. 226-2.

Article R. 226-8 of the French Criminal Code

Applications for authorisation must be submitted to the director general of the National Cybersecurity Agency (ANSSI). The application must include, for each type of device or technical equipment:

1. The name and address of the applicant, if a natural person, or its name and registered office, if a legal entity;

2. The type of device or technical equipment and the number of devices for which possession is requested;

3. The intended use;

4. A commitment to comply with the necessary inspections to verify the accuracy of the information provided in the authorisation application.

Article R. 226-9 of the French Criminal Code

The authorisation referred to in Article R. 226-7 is issued for a maximum period of three years.

It may impose conditions on the use of the devices or technical equipment to prevent misuse.

It is granted automatically to State agents or services for the acquisition and possession of devices or technical equipment they are authorised to use under the law.

Article R. 226-10 of the French Criminal Code

Holders of one of the authorisations referred to in Article R. 226-3 may only offer, transfer, rent, or sell devices or technical equipment listed under Article R. R. 226-1 to holders of an authorisation under Article R. 226-3, Article R. 226-7, or Article L. 34-11 of the French Postal and Electronic Communications Code.

They must keep a register recording all operations relating to this equipment. The template for this register is determined by order of the Prime Minister, issued following the opinion of the commission referred to in Article R. 226-2.

Article R. 226-11 of the French Criminal Code

The authorisations provided for in Article R. 226-3 and Article R. 226-7 may be withdrawn:

1. In the event of a false declaration or false information;

2. In the event of a change in the circumstances on the basis of which the authorisation was granted;

3. If the beneficiary of the authorisation fails to comply with the provisions of this section or with any specific obligations imposed by the authorisation;

4. If the beneficiary of the authorisation ceases the activity for which the authorisation was granted.

The authorisation may only be withdrawn, except in cases of urgency, after the holder has been given the opportunity to present their observations.

Authorisations shall automatically expire if the holder is convicted of any of the offences provided for in Articles 226-1, 226-15 or 432-9.

Article R. 226-12 of the French Criminal Code

Persons who manufacture, import, possess, exhibit, offer, rent, or sell devices or technical equipment listed under Article R. 226-1 must comply with the provisions of this section by applying for the necessary authorisations within three months from the publication of the order provided for under Article R. 226-1.

If authorisation is not granted, these persons have one month to destroy the devices or technical equipment, or to sell or transfer them to a person holding one of the authorisations provided for under Articles R. 226-3, R. 226-7, or Article L. 34-11 of the French Postal and Electronic Communications Code. The same applies if the authorisation expires or is withdrawn.

Order of 4 July 2012 establishing the list of devices and technical equipment provided for under Article 226-3 of the French Criminal Code

Article 1

The list of devices and technical equipment subject to the authorisation referred to in Article R. 226-3 of the French Criminal Code, as provided for in Article R. 226-3 of the same Code, is set out in appendix I to this order.

Article 2

The list of devices and technical equipment subject to the authorisation referred to in Article R. 226-3 of the French Criminal Code, as provided for in Article R. 226-7 of this Code is shown in Appendix II to this Order.

Article 3-1

This order applies throughout the territory of the Republic.

Article 4

The director general of the National Cybersecurity Agency (ANSSI) is responsible for implementing this order, which will be published in the Official Journal of the French Republic.

Order of 16 August 2006 concerning the register referred to in Article R. 226-10 of the French Criminal Code

Article 1

The register referred to in Article R. 226-10 of the French Criminal Code, recording all operations relating to the equipment listed in the order of 29 July 2004, complies with the model set out in the appendix to this order *[Order repealed and replaced by the order of 4 July 2012.]*.

Article 2

This register takes the form of a bound and initialled ledger, maintained by the head of the company that has undertaken to comply with the necessary inspections as provided for under Article R. 226-4 of the French Criminal Code.

Article 3

The order of 15 January 1998 on the same subject is hereby repealed.

Article 4

This order will be published in the Official Journal of the French Republic.

Photo credits: H. Véronèse/Centre Pompidou/Patrick Gaillardin/Léo-Paul Ridet/Sorbonne Université/Florian Guigui.

Hôtel de Cassini - 32 rue de Babylone - 75007 Paris
https://www.cnctr.fr/

Design: DSAF / DPSG / BAEC / Section Édition – Printing: Baudelaire – October 2025 - ISSN 2268-5278.