CNCTR

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

10th Activity Report 2025

FOREWORD 7

2025 ACTIVITY REPORT 17

Summary 19

2025 Key figures 24

Part 1. *Ex ante* control 27

1.1. A reminder of the framework for surveillance and its oversight 27

1.2. The number of people under surveillance 31

1.2.1. 25,332 people have been under surveillance in 2025 31

1.2.2. Change in the number of people under surveillance in recent years 33

1.2.3. Following the Olympic year, the focus on preventing organised crime is once again at the forefront of the surveillance activities carried out in 2025 35

1.2.4. The issue of surveillance relating to separatism and entrism 36

1.3. Requests for intelligence-gathering techniques 38

1.3.1. Over 100,000 requests submitted to the Prime Minister in 2025 38

1.3.2. Breakdown of requests by purpose 39

1.3.3. Breakdown of requests by intelligence-gathering technique 43

1.3.4. The specific issue of developments in the collection and recording of computer data 47

1.3.5. Algorithm and the surveillance of international electronic communications 49

1.4. Unfavourable opinions and requests for further information 50

Part 2. *Ex-post* control 53

2.1. Overview of the framework for *ex post* oversight 53

2.1.1. The aim of *ex post* oversight is to ensure that the intelligence services are aware of and comply with the legal framework governing the techniques they employ 53

2.1.2. The planning and allocation of oversight tasks amongst intelligence services form part of the general control policy 54

2.1.3. Control is a matter of teamwork, quality of preparation and execution, and dialogue 55

2.2. 120 *ex post* controls carried out in 2025 58

2.2.1. Trend in the number of controls over time 58

2.2.2. Two significant advances, achieved with the assistance of the intelligence services 58

2.3. Anomalies detected 61

2.4. 105 complaints in 2025 64

2.4.1. Reminder of the legal framework 64

2.4.2. Trends in the number of complaints 66

2.4.3. Average time taken to process complaints 66

2.5. The number of appeals brought before the Council of State remains very low 67

Part 3. Overview, challenges and perspective 68

3.1. An outward-looking approach 68

3.2. Unchanged resources 70

3.3. The CNCTR highlights the fact that two issues remain unresolved: the lack of a regulatory framework governing exchanges between French and foreign intelligence services, and the issue of 'sovereignty files' 72

3.3.1. The lack of a regulatory framework governing exchanges between French and foreign intelligence services 72

3.3.2. The issue of 'sovereignty files' 74

3.4. Among the areas requiring vigilance, algorithms and cryptanalysis occupy a prominent place 75

3.4.1. Algorithm: a missed opportunity in 2025, which offers a chance for greater security and clarity 76

3.4.2. Communications encryption: a step forward for the right to privacy, a challenge for intelligence services in a democratic state 80

STUDIES 85

Study 1. The principle of proportionality 87

Study 2. *Ex-post* control as described by those involved 95

APPENDICES 127

Changes in the composition of the college during 2025 129

Glossary 132

Foreword

2025, the year of the tenth anniversary of the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR), marked by the passing of Serge Lasvignes

Two events defined the CNCTR's year in 2025. They are very different, yet their impact is comparable.

Serge Lasvignes, Chairman of the CNCTR from October 2021 to 31 January 2025, died on 15 February 2025. Following our 2024 activity report, this report pays a final tribute to him[1]. The members of the Commission's board and staff intend to uphold and carry forward his example as a servant of the rule of law, his ability to maintain the balance, –which the law has entrusted this body with the responsibility of safeguarding,– between the protection of the Nation's fundamental interests and the defence of privacy and freedoms, and his rigorous yet trusting approach to dialogue with intelligence services.

Established by the Intelligence Act of 24 July 2015, the CNCTR began its work on 3 October of the same year. A symposium was held at the 'École Militaire' on 22 September 2025 to mark the commission's tenth anniversary[2]. The symposium brought together intelligence service officials, legal experts, elected representatives and journalists to examine, on the one hand, the principle of proportionality –which, alongside the principle of necessity, is one of the two pillars underpinning the implementation of public intelligence policy in France– and, on the other hand, the question of whether the CNCTR had effectively fulfilled its remit and remained capable of doing so. A 'ten-years compendium', published alongside this report, contains the proceedings of this symposium and testimonies from numerous stakeholders, in particular the drafters of the legislation and senior figures from the French intelligence community. Furthermore, this report

1. See also: 'A Humanist in the Service of the State – A Tribute to Serge Lasvignes', a publication by the Council of State, the General Secretariat of the Government and La Documentation française, March 2026.
2. The proceedings of this conference are available on the CNCTR's website under the 'Our events' section.

includes a summary of the presentation given by President Jean-Marc Sauvé at the symposium on 22 September 2025 concerning the principle of proportionality (Study No. 1).

In reviewing the activities of this unusual year, this tenth report reaffirms the CNCTR's commitment to fulfilling its remit.

A supervisory role in the service of acting as a guarantor

The word 'oversight' appears in the commission's very name and unambiguously defines its remit. This day-to-day work is carried out, *ex ante*, through the examination of the 100,000 annual requests for the use of intelligence-gathering techniques, on which the commission is required to give an opinion to the Prime Minister, and *ex post*, through the conduct of 120 annual inspections of the intelligence services of both circles[3]. The first and second parts of this report, as in every year, provide an account of this. Furthermore, a study complements the report on *ex post* oversight activities in a practical manner, by comparing the perspectives of the CNCTR's team and those of agents from several intelligence services on the conduct and benefits of these operations (Study No. 2).

This remit often leads to the CNCTR being described as the 'policeman' of intelligence services. The commission does not endorse this description, as it is inaccurate. The reason is simple and can be expressed in the same terms as those that led to this oversimplification: there is no policeman because there are no thieves. The CNCTR's day-to-day counterparts are public services responsible for enforcing the law in the implementation of public policy.

Although it is not part of the French intelligence community, the CNCTR is linked to it by a shared requirement: that intelligence public policy be conducted lawfully. Whilst it is the responsibility of one body to act and of

3. The 'first circle' services are the specialised intelligence services, designated by Article R. 811-1 of the Internal Security Code: DGSE, DRSD, DRM, DGSI, DNRED and Tracfin. The other services, known as the 'second circle', are designated by Article R. 811-2 of the same Code. They comprise several national services and the corresponding regional services: DNRT, DNPJ, DNPAF, DGGN, DRPP and SNRP.

the other to oversee, both must do so in accordance with the same legal principles and in compliance with the same constitutional requirements.

The system can only be robust if these principles and requirements are shared and put into practice, first and foremost, by the intelligence services themselves. In other words, external oversight would have neither strength nor lasting effect in such a sensitive area if the Nation as a whole could not first rely on the intelligence services responsible for its security to act in accordance with the law and to carry out the internal oversight for which they are responsible. The CNCTR frequently asks the intelligence services for clarifications or changes to their working practices. It welcomes the results when they are achieved and encourages further progress. In every case, the key lies in the services' control over their own conduct and their acceptance of the idea that the law does not impose a constraint but confers strength.

As such, the CNCTR sees itself less as a 'producer of oversight' than as a guarantor. Its interventions, its observations and its ongoing dialogue with intelligence services, the National Intelligence and Counter-Terrorism Coordination and the Interministerial Control Group (GIC) are intended to provide the Nation with the necessary assurance that intelligence public policy is being properly conducted, whilst offering the necessary nuances, criticism or encouragement as appropriate.

This report sets out, once a year, the circumstances in which the commission has carried out its duties, the findings it has drawn from its controls, and its views on a number of topical issues. More frequently, the CNCTR submits its analyses to Parliament, particularly during hearings. As the representative of the people and the maker of the law, Parliament must be able to assess how public policies are being implemented, including those relating to intelligence. The particular importance of the Parliamentary Intelligence Committee must be emphasised. This body is in regular contact with the intelligence community and the commission and cannot be subject to national defence secrecy rule. It therefore has a role as a trailblazer, to which the CNCTR owes its full support.

Limitations of various kinds, all of which call for progress

The law has defined the scope of the CNCTR's remit, tasking it specifically with monitoring intelligence-gathering techniques and not the intelligence services themselves, nor those aspects of their operations that do not rely on such techniques.

This definition is not at issue here. However, other limitations arise, some practical, others legal. These are likely to affect not only the commission's remit but also that of the intelligence services.

Firstly, this report highlights, more emphatically than previous ones, the CNCTR's shortage of staff and the risks this entails. Comprising a team of twenty-two staff members, fourteen of whom are responsible for *ex ante* and *ex post* oversight tasks, and with a nine-member board, five of whom are dedicated to this remit, the CNCTR considers itself to be operating at the limits of its capacity.

Its staffing levels have not kept pace with either the growth in its workload or the allocation of additional resources – both human and technical – to intelligence services.

The issue is far from being limited to the number of opinions the commission issues or the inspections it is required or able to carry out. It concerns the reality and sincerity of the assurance it is tasked with providing. Whilst the professional calibre and multidisciplinary nature of the commission's team are crucial, the commission will not be able to fulfil its remit for much longer without additional support, given the high level of technical expertise required and the need for a detailed understanding of the work carried out by the services themselves, which are responsible for preventing ever more diverse and growing threats.

Secondly, this report once again highlights a shortcoming and ambiguity in the French legal framework, which is, incidentally, of a high standard and remains effective ten years after its introduction.

The shortcoming lies in the absence of any framework governing the exchange of intelligence between French services and their foreign partners. Such exchanges are legitimate and, at times, vital. It is nonetheless necessary to reiterate that a framework is essential, one based on principles rather than formalities. The case law of the European Court of Human Rights requires this, and many countries have such a framework in place. This shortcoming is exacerbated by the fact that the law prohibits both the commission and the Parliamentary Intelligence Committee from knowing of such exchanges.

The ambiguity concerns so-called 'sovereignty files', which have no precise legal definition but which the French intelligence community places outside the legal framework of the Act of 24 July 2015 and which the intelligence services intend to keep away from the commission's oversight. Intelligence work draws on many other tools besides the techniques provided for by the Internal Security Code. It is neither the remit nor the intention of the CNCTR to pass judgement on the use of such other tools, nor on the effectiveness of the intelligence services' operations, nor on the strategy assigned to them by the Government. However, insofar as such 'sovereignty files' contain data collected by means of intelligence-gathering techniques, the commission must be able to access this data – and this data alone – in order to exercise its statutory oversight, which relates in particular to the retention period of the data, its actual relevance to the purpose that justified the use of the intelligence-gathering techniques, and its indispensability to the investigation. It is necessary to resolve this ambiguity and to determine the legal and technical means of extracting such data from 'sovereignty files' so that they may be subject to the commission's scrutiny.

Algorithmic techniques and the encryption of communications: topics of debate in 2025

The technique provided for in Article L. 851-3 of the Internal Security Code, known as the 'algorithm', is unique. Whilst not constituting mass surveillance, it makes it possible to detect individuals posing a threat, or their behaviour, which other techniques -all of which rely on the initial targeting of an individual- would be unable to identify. However, in its decision of 12 June 2025 on the law aimed at freeing France from the trap of drug trafficking, the Constitutional Council ruled that the inclusion in this technique of the full addresses of internet resources[4] –permitted since 2021 but never yet used– was contrary to the Constitution. This data is of a mixed nature: it traces a connection but may also, due to its precision, indicate the content accessed. Its processing by an intelligence-gathering techniques is therefore likely to constitute a serious infringement of privacy. Without disregarding the safeguard provided by the end-to-end controls exercised over algorithms by the CNCTR[5], the Constitutional Council ruled that it was for the legislature itself to regulate its use. The commission welcomes the rewriting and improvement of Article L. 851-3 provided for in the draft bill updating the Military Programming Act[6], which is currently being debated in Parliament at the time of this report's publication.

The issue of communications encryption, for its part, has not yet been resolved.

Encryption is a key safeguard to the privacy of correspondence, for public bodies as well as for everyone else. However, its increasing use has made it an obstacle to investigation using traditional interception techniques and therefore an obstacle to the protection of the fundamental interests of the Nation. In 2025, two parliamentary initiatives sought to resolve this dilemma, taking opposing approaches.

4. Also known as 'URL': *Uniform Resource Locator*
5. See the study on this technique in the CNCTR's 2024 activity report
6. See the CNCTR Board's decision of 12 February 2026, available online at cnctr.fr

The first sought to oblige providers of encrypted communications to hand over their content in plain text to intelligence services. The second, by contrast, sought to prohibit any such access whatsoever.

Neither of these two provisions was based on an in-depth technical and legal study, nor do they succeed in striking the necessary balance between equally important imperatives. The CNCTR hopes that such work, entrusted to a Member of Parliament on a special assignment and placed on their agenda by the Parliamentary Intelligence Committee, will inform Parliament and the Government and identify a legally viable path forward. It emphasises that the current state of affairs is unsatisfactory, as the obstacle posed by encryption leads intelligence services to make ever-increasing use of the technique of collection and recording of computer data (RDI), for which the number of authorisations rose by 38 per cent in 2025 following a 27 per cent increase in 2024. However, this latter technique is no less intrusive than a justified and targeted decryption, as it should be for any intelligence-gathering technique.

Significant progress and improvements in the management of the legal framework

The year 2025 saw two significant developments which the CNCTR wishes to commend.

On the one hand, a service of the first circle has enabled the commission's staff to receive training in the use of the data query tools employed by the services themselves. This access is essential for the commission to effectively exercise its oversight in particular of the international communications surveillance technique, which involves large volumes of data.

Furthermore, another department within the first circle has responded favourably to the CNCTR's request to monitor the situation from its own premises rather than only on-site for certain applications of

the collection and recording of computer data technique mentioned above. This is a positive step forward which paves the way for the introduction of a more comprehensive system for the remote monitoring of this technique, as decided by the President of the Republic at the end of 2023. This project is being led by the National Intelligence and Counter-Terrorism Coordination and by the General Secretariat for Defence and National Security. The first results are expected by mid-2027.

In addition to these advances, the commission noted in 2025 that the intelligence services had made improvements in their compliance with the legal framework established ten years earlier. It particularly emphasises the attention paid to its observations by the services from the second circle and, across the board, an effort to remedy, through internal oversight and training, any remaining shortcomings in implementation.

To promote these improvements and play its full part in them, the CNCTR decided at the end of 2025 on a number of measures which will be implemented during 2026. These include the appointment of a lead contact for each department, the strengthening of the coordination of *ex post* controls, the definition of an control policy, and an increased focus on the commission's development of guidance, where necessary following legal consultations with the departments.

Vincent Mazauric
State councillor,
chairman of the CNCTR

2025 Activity Report

Summary

The legislature has entrusted the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR) with the task of ensuring that the activities of the French intelligence services on national territory comply with the legal framework.

The commission's oversight, which aims to balance security and civil liberties and to protect citizens' fundamental rights, helps to uphold the rule of law and ensure legal certainty in the activities of the intelligence services, with whom it liaises on a daily basis.

It essentially takes two forms.

At the preliminary stage, the commission submits a preliminary opinion to the Prime Minister on each request to use intelligence-gathering techniques on national territory: this constitutes *prior* scrutiny. The commission is required to give its opinion within twenty-four hours where a request falls within the remit of a member who is a judge[7] [8] and ruling alone. This time limit is extended to seventy-two hours where the request requires consideration by a collegial panel, either in plenary or restricted session[9]. The commission adheres to these time limits; it may reach a decision more quickly under a so-called 'priority' procedure established to meet operational needs requiring urgent processing of requests[10].

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

8. Unless otherwise stated, the articles referred to in this report are those of the CSI.

9. Under the provisions of Article L. 832-3, the Commission's collegiate panels have exclusive jurisdiction to hear certain categories of applications (applications concerning regulated professions, to be heard by the full Commission; applications for admission to a private residential premises, to be heard by a select panel) and are also required to consider any new or serious issues.

10. This procedure enables the Commission to issue opinions within a timeframe generally of less than one hour.

Downstream, the CNCTR ensures, through inspections carried out partly on the premises of the intelligence services and partly from the Commission's own premises, that the legal requirements are complied with in the implementation of the authorisations granted by the Prime Minister: this is known as *ex post* monitoring. Each year, the number of *ex post* inspections that the commission is required to carry out is set when the Finance Act is passed[11].

This report has been drawn up in accordance with the provisions of Article L. 833-9 of the Internal Security Code (CSI). The statistical data contained therein are derived from a process of data extraction and aggregation carried out by the CNCTR in conjunction with the Interministerial Control Group (GIC), followed by data validation.

***

In 2025, 25,332 individuals were subject to surveillance and 100,813 requests for the use of domestic intelligence-gathering techniques were submitted to the CNCTR for its opinion before being presented to the Prime Minister for approval.

This represents a modest increase compared with 2024: 24,308 people under surveillance and 98,883 requests for the use of intelligence-gathering techniques.

Following an increase in the number and proportion of people placed under surveillance for the purposes of preventing terrorism in 2024, linked to the organisation of the Olympic and Paralympic Games in Paris, these figures fell in 2025. The number and proportion of people under surveillance for the purpose of preventing damage to the republican form of government, actions aimed at maintaining or reconstituting dissolved groups, or for the purpose of preventing Incidents of collective violence likely to seriously harm public peace

11. This is a target set out in the annual performance plan for Programme 308.

are also on the decline. Conversely, the number and proportion of people under surveillance for the purposes of preventing organised crime are rising.

The question has arisen as to whether individuals should be monitored on the grounds that they are pursuing a strategy of 'Entrism'. This is an important and sensitive issue. According to the Minister of the Interior, Entrism refers to a form of separatism characterised by a strategy of concealment[12]. The commission notes that, having regard, on the one hand, to this definition and, on the other hand, to the criminal offences to which –as the Constitutional Council has pointed out[13]– the prevention of attacks on the republican form of the government refers, the surveillance of a person solely on the grounds of entrism cannot be justified on the basis of the purpose of preventing attacks on the republican form of the government.

The breakdown of requests by type of technique shows that traditional techniques, such as security interceptions, have remained relatively stable, whilst there has been an even more marked increase than in the previous year in requests for more intrusive techniques, particularly the collection and recording of computer data (+27.2 per cent in 2024, +38.2 per cent in 2025).

The use of this technique, made necessary by the growing use of encrypted messaging services, calls for consideration of both the conditions under which it is used and the issue of encryption.

The commission also carried out 120 inspections to ensure that the authorisations granted by the Prime Minister were being properly implemented. Over the past year, it has focused its efforts on gaining a better grasp of the technical aspects of intelligence. The commission

12. Commission of Inquiry into the links between representatives of political movements and organisations and networks supporting terrorist activity or propagating Islamist ideology, National Assembly, 18 November 2025, statement by the Minister for the Interior.

13. Decision No. 2015-713 DC of 23 July 2015, point 10.

could not have achieved this improvement without the active support of the intelligence services. It welcomes this cooperation and progress, which stem from the intelligence services taking on board the observations made by the commission and set out, in particular, in its 2024 activity report.

It is not paradoxical that, in this climate of cooperation, more rigorous scrutiny should bring to light a greater number of anomalies. As part of our commitment to continuous improvement, 2026 must see ongoing improvements in the identification and resolution of these anomalies. Key factors underpinning these improvements include the sustained efforts by the intelligence services to manage risks, as well as the commission's teams' growing technical expertise and their increasing proficiency in using the data-processing systems available to the services.

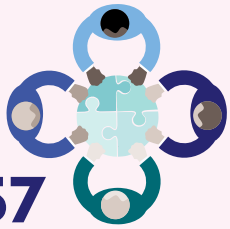
Despite an increase in its workload –comprising more requests, the growing technical complexity of processing these requests, and a constant number of checks that are becoming ever more thorough– the commission has fulfilled its remit with the same resources. In 2025, it found itself at the limits of its capacity. The commission considers that the alert threshold has been reached.

2025 Key figures

100,813
requests for intelligence-gathering techniques
(individual domestic techniques)[14]



25,332
people under surveillance



157
collegial meetings

120
controls
within the intelligence services



€3.4 million
budget

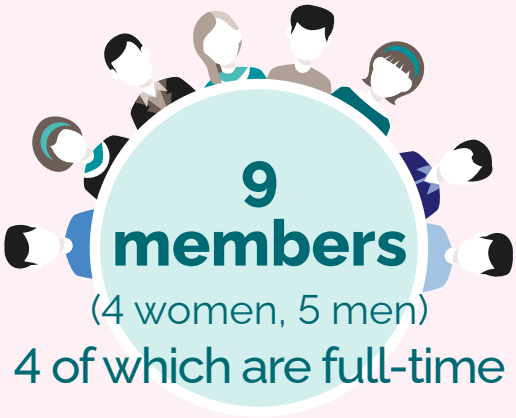


14. This data does not include non-individualised requests and/or requests relating to international electronic communications surveillance measures which covers requests relating to the technique known as the algorithm provided for in Article L. 851-3 of the French Internal Security Code, requests for 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 p. 49 below).

10 trips to the territories, including **1 overseas** department



On 31 December 2025:



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

22 staff

- 11 women / 11 men
- 12 public agents / 10 contract agents
- Average age of 40 years

Part 1. *Ex ante* control

1.1. A reminder of the framework for surveillance and its oversight

The conditions under which persons present on national territory may be subject to surveillance using intelligence-gathering techniques within the framework of administrative policing –that is to say, as a preventive measure– have been laid down by the legislature in the Internal Security Code (CSI).

Intelligence services may be authorised to use intelligence-gathering techniques to defend and promote certain fundamental interests of the Nation. Article L. 811-3 of the CSI states:

- under purpose 1, National independence, territorial integrity and national defence;
- under purpose 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;
- under purpose 3, the major economic, industrial and scientific interests of France;
- under purpose 4, the prevention of terrorism;
- under purpose 5, the prevention of: (a) damage to the republican form of government; (b) actions aimed at maintaining or reconstituting dissolved groups pursuant to Article L. 212-1 of the CSI; (c) collective violence likely to seriously harm public peace;

- under purpose 6, the prevention of organised crime and delinquency;
- under purpose 7, the prevention of the proliferation of weapons of mass destruction.

The defence and promotion of these fundamental interests shall hereinafter be referred to, respectively, as 'purpose 1', 'purpose 2', 'purpose 3', 'purpose 4', 'purpose 5a', 'purpose 5b', 'purpose 5c', 'purpose 6' and 'purpose 7'.

Furthermore, a specific purpose of the National Prison Intelligence Service, as set out in Article L. 855-1 of the CSI, is to prevent escapes and to ensure security within prisons or healthcare facilities intended to accommodate detainees. This shall be referred to as 'purpose L. 855-1'.

The first question the CNCTR must ask itself when examining an application is whether surveillance is necessary. Is there a link between the person concerned and the purpose cited by the service that makes it necessary to use an intelligence-gathering techniques to prevent a threat? This assessment is carried out on the basis of the grounds set out by the service. The Commission may ask the service to clarify these grounds by requesting further information.

The second question concerns the proportionality of the proposed technique. The CSI sets out an exhaustive list of the techniques that may be used[15]. Some are long-established, such as security interceptions (which include telephone 'tapping'), whilst others are more recent, such as the collection and recording of computer data (RDI) provided for by Article L. 853-2 of the CSI. They vary in their degree of intrusiveness: accessing the telephone numbers that have been in contact with a person does not invade privacy in the same way as, for example, the recording of sound or images.

15. See the factsheet on the various intelligence-gathering techniques: https://www.cnctr.fr/techniques-de-renseignement.

A third question concerns, where applicable and when provided for by law, the subsidiarity of the technique under consideration. The most intrusive techniques – such as the recording of words spoken in a private capacity and the recording of images in a private setting, or the collection and recording of computer data – are justified only '*where the information cannot be obtained by any other legally authorised means*' (Articles L. 853-1 and L. 853-2).

Each technique may be authorised by the Prime Minister only for a limited period: four months for the least intrusive techniques, and two months or even thirty days for the most intrusive ones. The authorisation may be renewed upon a reasoned request from the relevant service, subject to the same time limits.

It should be noted that a person may be the subject of several requests for intelligence-gathering techniques at the same time; the CNCTR issues an opinion on each of these requests but takes their cumulative effect into account in its assessment of proportionality.

An important criterion for proportionality is the duration of the surveillance. Whilst the service may lawfully request the renewal of an authorisation granted for the period specified above, the extension of the surveillance must be justified by the continued existence of the risk or threat posed by the person concerned. This assessment is a delicate one for both the intelligence services and the commission. Indeed, it is the very nature of administrative policing – which is preventive by nature, as opposed to criminal investigation – to be subject to uncertainty.

Having weighed up the need to prevent an infringement of the nation's fundamental interests against the protection of citizens' fundamental rights, the commission is not obliged to accept or reject *en bloc* all applications relating to the same person.

In the light of the evidence submitted to it, it may issue a favourable opinion on the use of one particular technique, such as a security interception, and an unfavourable opinion on the use of another technique which it considers too intrusive in the light of the evidence presented by the intelligence service.

For example, the commission may consider that requests for real-time geolocation and security interception are proportionate to the risks and grounds cited by the service, but that this is not the case for a request to collect computer data on the same person until the former techniques have substantiated the initial grounds.

It may also attach conditions to its favourable opinion, in particular regarding the duration of the measure, by setting a period shorter than the statutory maximum. A typical example of such a restriction is an application relating to a specific event: once that event has passed, there will no longer be any justification for monitoring individuals whom were, in that context, considered to pose a risk or threat.

The year 2025 confirms the growing role of collection and recording of computer data. This is an intrusive technique, which the legislature has stipulated may only be used as a last resort, that is to say, on condition that other techniques fail to yield the required information. Its increasing use raises questions about how to maintain a satisfactory balance between the legitimate surveillance of certain individuals and the need to safeguard the rights of every citizen, in particular the right to privacy.

1.2. The number of people under surveillance

As it has done since its first activity report, the commission gives an estimate of the number of individuals whom, in 2025, were subject to at least one intelligence-gathering technique from among those provided for in Chapters I to III of Title V of Book VIII of the Internal Security Code. Authorisations for access to recorded connection data are not taken into account, as these are limited to enabling the identification of subscribers and the recording of subscription numbers[16].

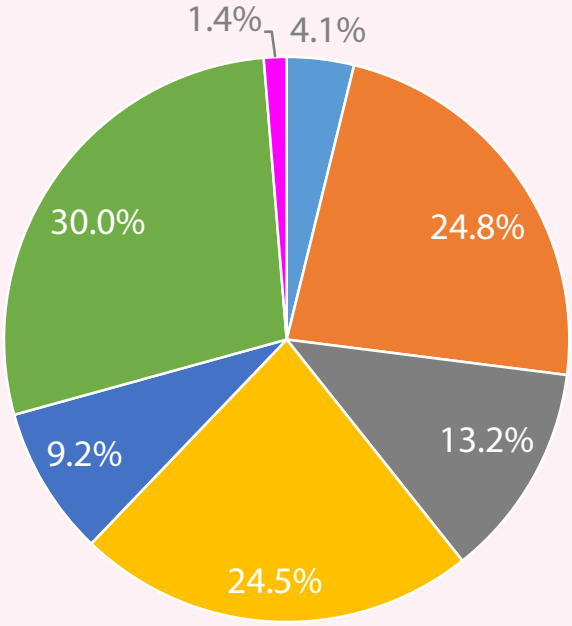
1.2.1. | 25,332 people have been under surveillance in 2025

The number of people under surveillance in 2025 stands at 25,332, with 30 per cent falling under purpose 6 and the remainder divided roughly equally between purposes 2 and 4.

The chart below shows the breakdown in detail.

16. The CNCTR considers that the identification of subscribers and the recording of subscription numbers, as provided for in the second paragraph of Article L. 851-1, constitute not so much surveillance measures in the strict sense as a prerequisite for such measures. In the Commission's view, surveillance measures commence as soon as 'itemised bills' for the person concerned are obtained pursuant to the first paragraph of the same Article L. 851-1.

Breakdown of persons under surveillance according to the purposes justifying their



- 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 France
- The prevention of terrorism
- The prevention of: a) Damage to the republican form of government; b) Actions aimed at maintaining or reconstituting 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 subject to surveillance for several purposes, the total of the percentages shown exceeds 100 per cent.

1.2.2. Change in the number of people under surveillance in recent years

25,332 people were under surveillance in 2025, an increase of 4.2 per cent compared with 2024 (24,308).

This increase of just over a thousand is largely due to improvements in the reliability of the estimation method. This enabled an error that had affected previous counts to be identified and corrected.

Had the 2025 count been carried out without this correction, the result would have been approximately 800 units lower and would have shown an increase of only 1 per cent compared with 2024.

The correction made falls within the 10 per cent margin of uncertainty that has been associated with this estimate from the outset (see, on this point, the 8th activity report, page 29, and the 9th activity report, page 32)[17]. The same error affected the figures for previous years, with a likely comparable impact, but it has not been possible to correct the figures for those years.

The year 2023 had seen a marked increase: 20,958 people under surveillance in 2022, 24,209 people under surveillance in 2023 -an increase of 15.5 per cent. In 2024, this figure rose only marginally: 24,308 people were under surveillance, despite exceptional circumstances. In 2025, if one disregards the correction mentioned above, the number of people under surveillance therefore appears to be stabilising or, at the very least, rising only very moderately.

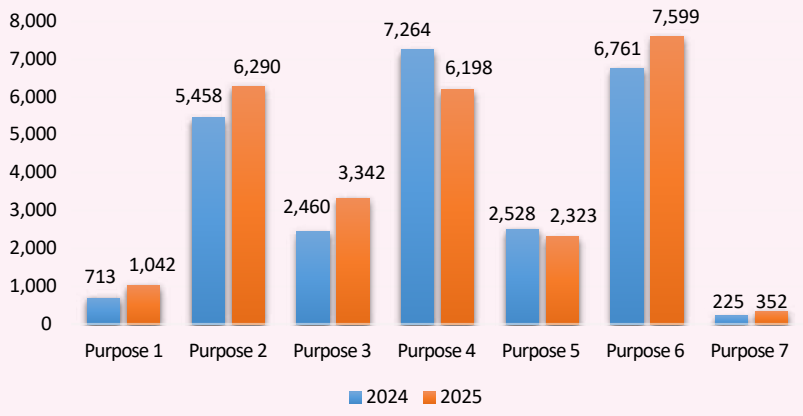
17. As highlighted in previous reports, the results of this calculation do, however, contain a margin of error due to various constraints. Indeed, the processing of requests for intelligence-gathering techniques involves the use of different software applications, which leads to the aggregation of data that is not, even today, fully harmonised. Furthermore, requests from the services are categorised by the intelligence-gathering technique specified in the Internal Security Code, rather than by individual. Moreover, the individuals concerned are not always identified by name or precisely identified.

Against this tense backdrop, this demonstrates the maturity and sense of responsibility shown by the intelligence services in their use of the resources made available to them. This stability is equally indicative of the persistence of threats of all kinds at a level that shows no sign of abating.

	2021	2022	2023	2024	2025*	2024/2025 Change	2021–2025 Change
Number of persons under surveillance	**22,958**	**20,958**	**24,209**	**24,308**	**25,332**	**+4.2%**	**+10.3%**
For terrorism prevention purpose	**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)	**6,198** (24.5% of the total)	**-14.7%**	**-20.8%**
For purpose linked to the prevention of organised crime and delinquency	**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)	**7,599** (30% of the total)	**+12.4%**	**+28.1%**
For the purposes provided for in Article L. 811-3 (5) of the French Internal Security Code	**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)	**2,323** (9.2% of the total)	**-8.1%**	**-33%**

*2025: refinement of the calculation method.

People under surveillance by purpose 2024–2025



1.2.3. Following the Olympic year, the focus on preventing organised crime is once again at the forefront of the surveillance activities carried out in 2025

In 2024, against the backdrop of the organisation of the Paris 2024 Olympic and Paralympic Games, part of the services' work had been refocused on the purpose of preventing terrorism, which had resulted in an increase in the number of people under surveillance to this end. The number of people under surveillance under purpose 4 fell by 14.7 per cent between 2024 and 2025, this decline reaching 20.8 per cent over the 2021–2025 period.

As in 2024, the number of people monitored under purposes 5a, 5b and 5c has fallen: by 8.1 per cent, following a decline of 0.9 per cent in 2024 and of 5.2 per cent in 2023. This figure is at its lowest level since 2018[18]. The CNCTR points out that purpose 5c is the most difficult to assess, both for the services and for the supervisory authority[19], as it lies at the intersection of the fundamental freedoms of opinion, expression, association and demonstration. A reduction in the use of this purpose alleviates the difficulties involved in assessing it.

By contrast, surveillance carried out under purpose 6 – which mainly concerns the risk of breaches of narcotics legislation – has once again become, as in 2023, the leading reason for surveillance in terms of the number of people concerned. This corroborates the commission's observation in its 2023 activity report that 'the threat posed by drug trafficking has now become a challenge to the normal functioning of institutions'[20]. The legislature sought to address this by passing the Act of 13 June 2025 aimed at freeing France from the trap of drug trafficking.

18. 2,116 people were under surveillance on these grounds in 2021 (CNCTR's 6th activity report for 2021, p. 73).
19. See the study on this issue in the 2022 activity report, p. 75
20. See the 2023 activity report, p. 12

In light of this purpose, the CNCTR emphasises the need to ensure compliance with the constitutional separation of powers between the administrative and judicial authorities. Indeed, whilst administrative surveillance may be entirely justified where there is a suspicion that a crime or offence may have been committed by an organised gang, it must cease without delay and be referred to the judicial authorities as soon as there is sufficient evidence to warrant judicial investigations aimed at establishing the offences and identifying the perpetrators with a view to their prosecution.

Surveillance activities under purposes 2 and 3 have increased in 2025, both in terms of the number of individuals concerned and as a proportion of the total. This trend reflects the growing threat posed by external factors of a geopolitical and economic nature.

1.2.4. | The issue of surveillance relating to separatism and entrism

Finally, 2025 saw an increase in the attention paid by public authorities to the phenomena known as 'separatism'[21] and 'entrism'[22].

An important question is whether surveillance using intelligence-gathering techniques can be carried out to identify, prevent or disrupt manifestations of these phenomena, which are very diverse and generally do not involve violence.

The Ministry of the Interior has carried out a review to determine whether the purposes set out in Article L. 811-3 of the CSI permit the use of intelligence-gathering techniques in cases of entrism[23]. He questioned the purpose set out in 5a, which concerns '*damage to the republican form of government*'.

21. See, in particular, the National Defence and Security Council (CDSN) meeting of 21 May 2025, chaired by the Head of State, which, with regard to separatism, reviewed three years of the law's implementation in upholding the principles of the Republic.
22. CDSN meeting of 7 July 2025, chaired by the Head of State, devoted to the fight against Islamism and the phenomena of separatism and entrism.
23. Committee of Inquiry into the links between representatives of political movements and organisations and networks supporting terrorist activity or propagating Islamist ideology, National Assembly, 18 November 2025, hearing of the Minister for the Interior.

Indeed, separatism has been defined as seeking to 'build small counter-societies separate from the national community'[24] rules, which concern the entire community of citizens'[25] and is characterised by a 'strategy of concealment'[26].

The commission neither underestimates nor downplays the reality of these phenomena nor the seriousness of their civic and social consequences.

It points out, however, that when examining the constitutionality of the Intelligence Act of 24 July 2015, the Constitutional Council noted[27] that the legislature had defined purposes 1 to 7 by reference to provisions of the Criminal Code or, in the case of purpose 5b, to Article L. 212-1 of the CSI, which refers to the Criminal Code.

In particular, the Constitutional Council has clarified that purpose 5a refers to the criminal offences set out in Chapter II of Title Ier of Book IV of the Criminal Code, relating to attacks (Article 412-1 of the Criminal Code), conspiracy (Article 412-2), insurrectionary movements (Articles 412-3 to 412-6), as well as usurpation of command, the raising of armed forces and incitement to arm oneself illegally (Articles 412-7 and 412-8).

Given the nature of the phenomena currently observable, separatism and entrism do not constitute any of the infringements of the Nation's fundamental interests referred to in these provisions.

Consequently, under current law, purpose 5a cannot form the basis for the surveillance of an individual on the grounds of separatism or entrism. This does not preclude the same individual from being placed under surveillance under other purposes provided for by the CSI if it is plausible that they intend to carry out or become involved in acts falling within the scope of those purposes.

24. Response from the Ministry of the Interior to topical question to the Government No. 0369G (Senate), given in a public sitting on 21 May 2025.

25. *Ibid.*

26. Committee of Inquiry into the links between representatives of political movements and organisations and networks supporting terrorist activity or propagating Islamist ideology, National Assembly, 18 November 2025, hearing of the Minister for the Interior.

27. Decision No. 2015-713 DC of 23 July 2015, paragraph 10.

1.3. Requests for intelligence-gathering techniques

1.3.1. Over 100,000 requests submitted to the Prime Minister in 2025

The number of requests submitted to the Prime Minister for the use of intelligence-gathering techniques within the country exceeded 100,000 in 2025, reaching 100,813[28] – an increase of 2 per cent compared with the previous year (98,883).

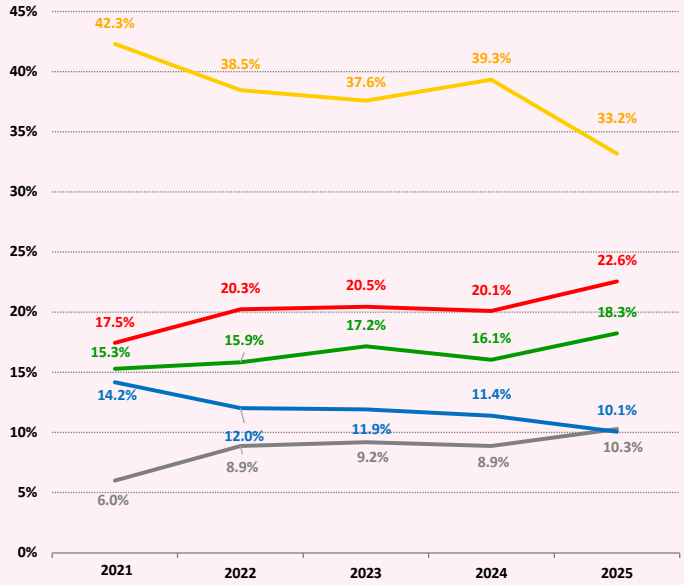
	2021	2022	2023	2024	2025	2024/2025 Change	2021/2025 Change
Number of requests submitted to the Prime Minister	**87,588**	**89,502**	**94,902**	**98,883**	**100,813**	**+2%**	**+15.1%**

Before being submitted to the Prime Minister, each of these requests was, following a review and within the time limits set out in 1.1, the subject of an individual opinion from the CNCTR.

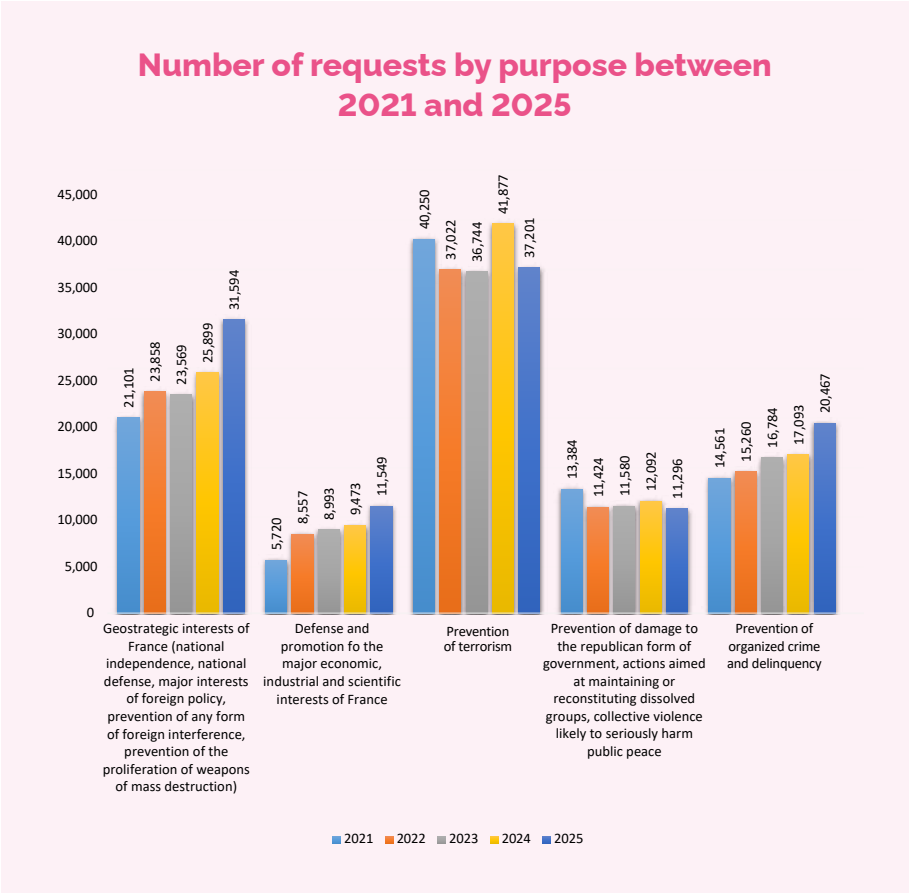
28. This figure covers individualised techniques and therefore does not include requests based on Article L. 851-3 (the so-called 'algorithm' technique), nor transfers between services covered by an authorisation from the Commission, nor international surveillance.

1.3.2. | Breakdown of requests by purpose

Number of requests by purpose between 2021 and 2025



- 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 France
- The prevention of terrorism
- The prevention of: a) Damage to the republican form of government; b) Actions aimed at maintaining or reconstituting dissolved groups; c) Collective violence likely to seriously harm public peace
- The prevention of organised crime and delinquency



29

Before making any comments, it should be noted that there is not, and cannot be, an absolute correlation between the trend in the number of individuals under surveillance for each purpose (1.2. above) and the trend in the number of techniques requested by the intelligence services for the same purposes. Indeed, both the number of techniques employed and the duration required for surveillance vary according to the operational circumstances specific to each risk and, therefore, to each purpose.

29. The 2024 activity report contains a similar chart on page 56. However, the caption for the first set of bar charts incorrectly stated 'France's geostrategic interests', corresponding to purposes 1, 2 and 7, whilst the figures shown related solely to 'major interests of foreign policy and the prevention of any form of foreign interference', that is to say, purpose 2.

However, even in the absence of such a correlation, the respective trends in the number of individuals and the number of techniques are consistent.

The year 2025 confirms the trend observed in recent years: a decrease in the proportion of applications submitted under purposes 4 and 5, and an increase in those submitted under purposes 2, 3 and 6.

Requests submitted for the purpose of preventing terrorism remain, both in absolute terms and as a proportion, the most numerous. However, following a slight increase in 2024 (+1.7 percentage point) due to the specific context of the Olympic and Paralympic Games, their proportion fell sharply in 2025 (-6.1 percentage points), confirming the trend observed over several years: they accounted for 42.3 per cent of all requests in 2021, compared with 33.2 per cent in 2025.

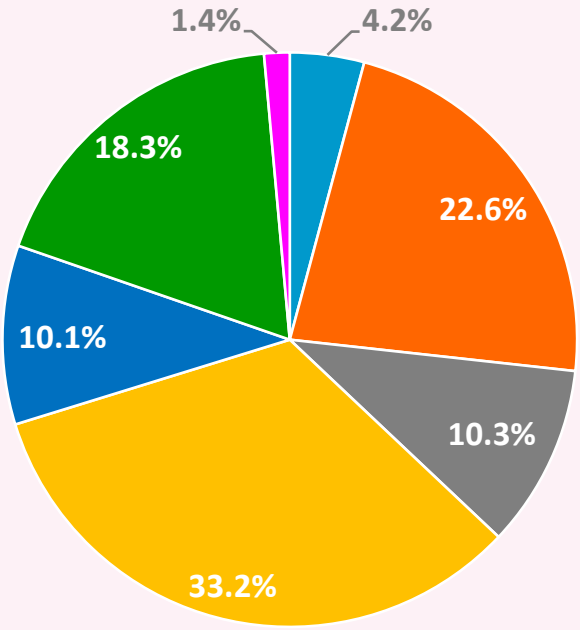
Applications submitted under purpose 5, across its various components, follow a similar trend, albeit a less pronounced one: with a fall of 1.3 percentage point in 2025, these applications account for 10.1 per cent of the total number of applications. In 2021, they accounted for 14.2 per cent of the total.

Conversely, applications submitted under purpose 2 and 3 continue to rise (by 2.5 percentage points and 1.4 percentage point respectively in 2025, representing 22.6 per cent and 10.3 per cent of the total, compared with 17.5 per cent and 6 per cent in 2021), in line with the current geopolitical context.

Similarly, applications submitted under purpose 6 rose significantly in 2025 (+2.2 percentage points, reaching 18.3 per cent of total applications). This confirms an underlying upward trend for the third legal basis invoked in support of applications for surveillance techniques. This trend is consistent with that observed in the number of individuals under surveillance.

The 'L. 855-1' purpose, specific to the prison intelligence service, gave rise to 125 requests in 2025, following 96 requests in 2024, 118 in 2023 and 110 in 2022.

Breakdown of purposes underlying all requests



- 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 France
- The prevention of terrorism
- The prevention of: a) Damage to the republican form of government; b) Actions aimed at maintaining or reconstituting dissolved groups; c) Collective violence likely to seriously harm public peace
- The prevention of organised crime and delinquency
- The prevention the proliferation of weapons of mass destruction

1.3.3. | Breakdown of requests by intelligence-gathering technique

The rise in the number of requests masks contrasting trends depending on the type of technique involved, with 'traditional' techniques remaining relatively stable but a marked increase in more intrusive techniques.

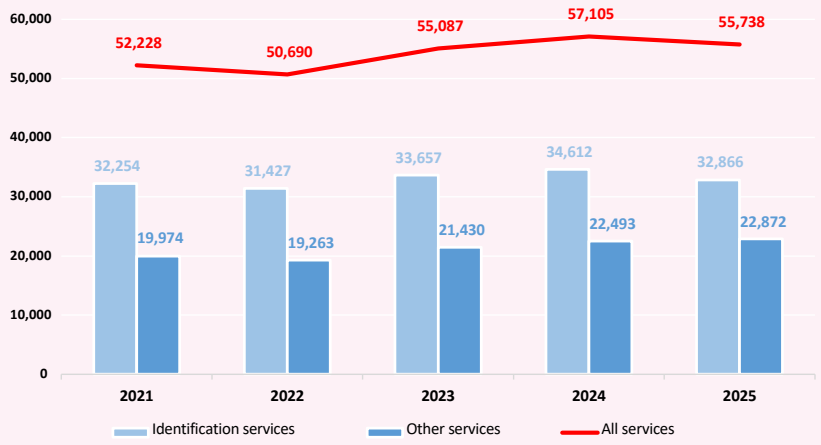
The number of requests for access to recorded connection data –a first-line surveillance technique enabling the authorities to establish the context in which the target operates[30]– remains broadly stable.

	2021	2022	2023	2024	2025	2024/2025 Change	2021/2025 Change
Access to recorded connection data (identification of subscribers and the index of subscription numbers) (Article L. 851-1)	32,254	31,427	33,657	34,612	32,866	-5%	+1.9%
Access to recorded connection data (other requests, including linked to 'phone records') (Article L. 851-1)	19,974	19,263	21,430	22,493	22,872	+1.7%	+14.5%
Real-time access to connection data (Article L. 851-2)	1,534	1,175	763	731	677	-7.4%	-55.9%
Real-time geolocation (Article L. 851-4 of the French Internal Security Code)	9,920	10,901	10,982	9,909	10,215	+3.1%	+3%
Security interceptions through the Interministerial Control Group (Article L. 852-1)	12,736	12,798	13,021	14,316	14,284	-0.2%	+12.2%
Tapped communications using *IMSI catcher* (II of Article L. 852-1)	0	0	0	0	0	-	-
Security interceptions on exclusively wireless networks (Article L. 852-2)	3	5	10	5	5	-	+66.7%
Collection of correspondence sent or received through satellite (Article L. 852-3)	0	0	0	1	8	+700%	-

30. See the 2023 and 2024 activity reports.

	2021	2022	2023	2024	2025	2024/2025 Change	2021/2025 Change
Location of people or objects ('geolocation devices') (Article L. 851-5)	2,006	1,951	2,084	2,065	2,317	+12.2%	+15.5%
Collection of connection data using *IMSI catcher* (Article L. 851-6)	583	641	607	616	678	+10.1%	+16.3%
Recording of words spoken in a private capacity and recording of images in a private setting (Article L. 853-1)	2,138	3,314	3,802	3,912	4,189	+7.1%	+95.9%
Collection and recording of computer data (Article L. 853-2)	3,758	4,260	4,493	5,715	7,900	+38.2%	+110.2%
Entering of private places (Article L. 853-3)	2,682	3,767	4,053	4,508	4,802	+6.5%	+79%
All requests for intelligence-gathering techniques	87,588	89,502	94,902	98,883	100,813	+2%	+15.1%

Change in the breakdown of requests for access to connection data between 2021 and 2025



The number of requests for security interceptions – which include, in particular, 'telephone tapping' – submitted to the Prime Minister stands at 14,284, virtually identical to the number of requests submitted the previous year: 14,316.

The capping of security interceptions requests by order of the Prime Minister contributes to this moderation.

Its primary function is to set a precise limit on the number of surveillance operations carried out at any given time, thereby protecting society from the risk of mass surveillance.

Furthermore, as it imposes a constraint on the intelligence services, the quota system serves as an effective incentive to carry out only the most essential surveillance operations and to refrain from initiating or extending those that are less justified. The quota is adjusted as necessary, following advice from the CNCTR, as was the case in 2025:

the security interception quota that could be carried out simultaneously, to 4,100, having been exceptionally increased to 4,500 for the duration of the Olympic and Paralympic Games.

The number of requests to collect correspondence sent or received through satellite remains very low: 8 requests in 2025, following 1 in 2024. This demonstrates that this technique, authorised on an experimental basis until 31 July 2025 by Act No. 2021-998 of 30 July 2021 on the prevention of acts of terrorism and intelligence, and subsequently until 31 July 2028 by Article 16 of Act No. 2025-532 of 13 June 2025 aimed at freeing France from the trap of drug trafficking, is still in its infancy[31].

By contrast, the number of requests for the recording of words spoken or images has risen by 7.1 per cent to 4,189 requests in 2025.

In particular, the number of requests for the collection and recording of computer data is expected to reach 7,900 in 2025, representing an increase of 38.2 per cent, following a 27 per cent rise in 2024.

Consequently, requests for entry into private places – which serve as a 'support' technique for certain intelligence-gathering methods – rose by 6.5 per cent, compared with 11.2 per cent last year. It should be noted that this latter trend is due in particular to the doubling of the authorisation period for entry into private places, as provided for in Article 17 of the Act of 13 June 2025. The increase from thirty to sixty days automatically leads to a reduction, in the event of prolonged surveillance, in the number applications for renewal.

This assessment confirms a fundamental trend identified by the CNCTR over several years: the increasing use of the RDI.

31. For further information on this technique, see the 2024 activity report, p. 48.

1.3.4. The specific issue of developments in the collection and recording of computer data

Between 2021 and 2025, the number of requests for digital evidence (RDI) more than doubled. As a subsidiary technique[32], RDI enables the collection and recording of all data from a digital device: computer, telephone, tablet, *etc*.

The number of RDI applications and their proportion of the total number of applications can be partly explained by the fact that the duration of authorisations for this technique is legally limited to two months, whereas that for security interception authorisations is four months. Consequently, assuming that both techniques are used in relation to the same person for eight months, subject to the authorisations being renewed, four RDI applications will have to be submitted, but only two security interception applications.

That said, this legal distinction and the quantitative effect it produces explain the number of RDI requests but not their increase.

The growth in the number of RDI applications, which has been ongoing for several years, reflects the gradual replacement of security interceptions by RDIs. In 2021, the number of RDI applications was equivalent to a quarter of the number of security interception applications. By 2025, this proportion had risen to more than half.

This trend reflects changes in communication methods. The use of the 'traditional' telephone is gradually being phased out in favour of other means of communication, in particular the use of end-to-end encrypted messaging services.

Faced with the obstacle of encryption, the authorities are compelled to resort to the use of RDI techniques, in addition to traditional methods.

32. I of Article L. 853-2 of the CSI.

A thorough review of the conditions under which this technique is used is called for.

A request for RDI, a subsidiary technique, normally follows requests for intelligence-gathering techniques that it is logical to use as a first resort. As the growing use of encrypted messaging renders traditional techniques ineffective, in practice it is necessary to submit several requests to achieve a single purpose. Consequently, on the one hand, the principle of subsidiarity to which RDI must abide tends to take a back seat to a certain degree of automation, and, on the other hand, the total number of requests for intelligence-gathering techniques increases.

Finally, there is no legal gradation in the collection and recording of digital data. A request for digital data collection and recording submitted by an intelligence service will relate to one or more of the target's devices, and the authorisation granted will permit the collection of all data contained on those devices. Unlike a security interception, which allows for the selection of conversations or exchanges of interest to the service, the collection and recording of electronic data is likely to gather a much larger volume of data across a much broader scope. It is therefore the responsibility of the service tasked with implementing this technique, under the commission's supervision, to retain only that data which has a genuine and plausible connection to the intended purpose. This places a burden on the intelligence service and constitutes an important area of scrutiny for the committee.

A thorough review of how this tool – which is now essential for preventing threats to the Nation – should be managed from both a legal and operational perspective, so that it can continue to be implemented whilst respecting everyone's rights, and that the principles of proportionality and subsidiarity remain what they should be: a concrete practice, rather than merely a legislative slogan.

1.3.5. Algorithm and the surveillance of international electronic communications

Two new authorisations for the implementation of automated processing, known as 'algorithms', as provided for in Article L. 851-3 of the CSI, were granted in 2025 following a favourable opinion from the CNCTR, bringing the total number of authorised algorithms to eight since this technique was made available to the intelligence services in 2015. One of these was discontinued in 2024.

The option to use this technique for purposes other than the prevention of terrorism was exercised for the first time.

Please refer to Part 3 of this report for an analysis of the key developments in 2025 relating to this technique.

Finally, the number of requests to exploit international electronic communications remained stable, with just over 4,000 notifications.

	2021	2022	2023	2024	2025	2024/2025 Change	2021/2025 Change
Number of opinions issued on the surveillance of international electronic communications	**4,374**	**3,715**	**3,981**	**3,942**	**4,055**	**+2.9%**	**-7.3%**

1.4. Unfavourable opinions and requests for further information

The rate of unfavourable opinions stands at 0.4 per cent in 2025.

The number of unfavourable opinions, across all intelligence-gathering techniques, has almost halved compared with the previous year: -44.3 per cent. This decrease is driven by the very significant fall (-61.4 per cent) in unfavourable opinions relating to intelligence-gathering techniques other than requests for connection data.

Over the same period, the number of requests for further information –in which the commission asks the service to provide additional details to support its request for intelligence-gathering techniques– fell by around 10 per cent, but remained at a high level: 2,939 requests for further information out of 100,813 requests for intelligence-gathering techniques, a figure comparable to that of 2023.

	2024	2025	2024/2025 Change
Technical connection data			
Opinions delivered	**57,105**	**55,738**	**-2.4%**
Requests for further information	**1,698** *(i.e. 3% of the total)*	**1,410** *(i.e. 2.5% of the total)*	**-17%** *(-0.5 percentage points)*
Unfavourable opinions	**261** *(i.e. 0.5% of the total)*	**238** *(i.e. 0.4% of the total)*	**-8.8%** *(-0.1 percentage points)*
Other intelligence-gathering techniques			
Opinions delivered	**41,778**	**45,075**	**7.9%**
Requests for further information	**1,609** *(i.e. 3.9% of the total)*	**1,529** *(i.e. 3.4% of the total)*	**-5%** *(-0.5 percentage points)*
Unfavourable opinions	**542** *(i.e. 1.3% of the total)*	**209** *(i.e. 0.5% of the total)*	**-61.4%** *(-0.8 percentage points)*
All intelligence-gathering techniques combined			
Opinions issued	**98,883**	**100,813**	**2.0%**
Requests for further information	**3,307** *(i.e. 3.3% of the total)*	**2,939** *(i.e. 2.9% of the total)*	**-11.1%** *(-0.4 percentage points)*
Unfavourable opinions	**803** (i.e. 0.8% of the total)	**447** (i.e. 0.4% of the total)	**-44.3%** *(-0.4 percentage points)*

The low rate of unfavourable opinions is neither a sign of a lack of vigilance on the part of the commission, nor of the intelligence services' flawless adherence to the legal framework.

The commission has drawn up guidelines on the use of intelligence-gathering techniques, which it circulates to the intelligence services.

It provides reasons for its unfavourable opinions when submitting them to the Prime Minister and explains them to the intelligence services during the inspections it carries out, at the services' headquarters and in the operations centres of the Interministerial Control Group[33]. These explanations naturally help to ensure that the circumstances which gave rise to an unfavourable opinion do not recur.

Furthermore, on the initiative of the services or at the request of the commission, presentations focusing on a particular event, an emerging risk or a specific use of a technique enable the intelligence services and the supervisory authority to share knowledge and analyses. They help to provide a framework for the use of intelligence-gathering techniques.

The combination of these tools –requests for further information, justification and explanation, and the sharing of knowledge and analysis– goes a long way towards preventing the risk of non-compliance with the legal framework.

Finally, an unfavourable opinion is not the only tool available to the commission for ensuring compliance with the legal framework.

By qualifying its favourable opinions, it is also able to recommend that the Prime Minister issue authorisations subject to restrictions designed to ensure their legality, in particular with regard to the principles of necessity and proportionality, without it being necessary to issue an unfavourable opinion.

This flexibility takes two forms.

33. For information on visit of GIC operational centres, see Part 2, p. 57.

The first concerns the balance between the evidence available to the department to justify its request and the principle of necessity. In the context of administrative policing, certainty cannot be expected; only evidence based on presumption, probability or plausibility. Such evidence may sometimes be tenuous, even though the target's background, environment or contacts may give cause for concern. The adjustment will then consist of issuing a favourable opinion 'once, to confirm the person's involvement in relation to the grounds for the request', thereby giving the service the opportunity to dispel any doubts. Where surveillance has continued without providing further grounds for the initial suspicions, the commission may state that it is issuing a favourable opinion 'once again to confirm the person's involvement in relation to the grounds for the request' and, finally, 'one last time…'.

This classification does not in all cases indicate a lack of tangible results from the surveillance. On the contrary, it may mean that sufficient evidence has been gathered for the law to require that the case be referred from the administrative policing to the judicial authorities. The commission will then state that it is issuing its opinion 'once again' or 'one last time' 'with a view to referral to the courts'. In particularly clear-cut circumstances, the commission will specify that 'the Internal Security Code cannot be applied', once evidence of a crime or offence has been gathered. The opinion will then be unfavourable.

The second form of modulation relates to the principle of proportionality. In such cases, the commission will, having regard to the circumstances set out, recommend that the authorisation be subject to restrictive conditions, at least until initial investigations have confirmed the threat or risk. For example, a restriction might stipulate that surveillance be authorised for a period shorter than the statutory duration, or that, of the intelligence-gathering techniques envisaged by the service, only the least intrusive be permitted initially, or that a person be monitored on the grounds that he's part of the primary target's entourage[34].

34. On the issue of entourage, see the 2023 activity report, p. 117.

Part 2. *Ex-post* control

2.1. Overview of the framework for *ex post* oversight

2.1.1. The aim of *ex post* oversight is to ensure that the intelligence services are aware of and comply with the legal framework governing the techniques they employ

The CNCTR's control form part of a comprehensive plan that takes into account several elements setting out the commission's control policy. These controls take various forms: data controls, particularly regarding traceability, and file controls. They cover distinct areas -domestic or international– and are carried out using a range of methods tailored to their purpose: on-site or remote controls.

The minimum number of controls is determined each year by the legislature in the annual performance plan annexed to the Finance Act. For 2025, this number was 120. *Ex-post* controls within the intelligence services focus in the first place on data collected using intelligence-gathering techniques. How and when was it collected? How was it stored? How was it analysed? Was data for which the statutory retention period had expired destroyed? Full and accurate traceability of these operations forms the basis of these controls.

To answer these questions, the control team must have the technical expertise required to navigate multiple IT systems, but also the legal expertise required to understand how these tools implement the relevant provisions of the CSI.

Ex post review also covers individuals subject to surveillance measures. Placing individual surveillance within a broader context and, together with the relevant intelligence service, assessing the outcome of a long-term operation: these are all ways of assessing, from a fresh perspective, the proportionality of the intelligence-gathering techniques used, or even the necessity of surveillance measures which, during the *preliminary* review, had been the subject of an internal report or a qualified opinion[35], reflecting concerns that had arisen following a collegial discussion. This is known as 'case file review'.

Finally, *ex post* oversight may relate to international surveillance. In such cases, it is carried out in accordance with procedures tailored to the specific legal framework governing this type of surveillance, whilst taking into account the particular technical nature of the means employed.

2.1.2. The planning and allocation of oversight tasks amongst intelligence services form part of the general control policy

Unlike the *ex ante* review of all requests submitted by the intelligence services, *ex post* inspection cannot be exhaustive. It is necessarily selective. This selectivity must serve the CNCTR's fundamental purpose: to provide the public with the most reliable guarantee possible that public intelligence policy is conducted in accordance with the law.

To this end, the commission's overall monitoring plan takes several factors into account, in particular: new issues that have arisen, for example, during visits to GIC operating centres[36]; long-term surveillance operations, which require regular review of their justification, particularly in light of the principle of proportionality; surveillance operations concerning individuals holding a protected office or practising a protected profession; and circumstances in which either

35. For further details on qualified opinions, see Part 1, page 51.
36. For further details on these visits, see below, p. 57.

the commission or the relevant intelligence service may have encountered legal or technical difficulties, in order to verify that these have been resolved.

The commission's primary concern is to ensure that inspections are properly distributed across the intelligence services. It does not disclose the number of inspections carried out in each first -or second-circle service. However, as might be expected, this number depends on the volume of activity of each service. Every intelligence service, regardless of its size and volume of activity, is inspected annually by the CNCTR.

The commission also strives to maintain a balance between the different types of control –covering data, individuals under surveillance and international surveillance– which require different legal and technical expertise.

2.1.3. Control is a matter of teamwork, quality of preparation and execution, and dialogue

CNCTR inspections are led by a member of the commission's board and carried out by two or three team members.

Although the legislation does not rule out the possibility of an unannounced inspection, should this be necessary, all inspections are scheduled and notified to the service concerned several weeks in advance, and their detailed programme several days in advance, so that this service can mobilise the necessary expertise.

Careful preparation by the commission member and the relevant team members is essential for meaningful and effective discussions with the service during the oversight visit. The agenda drawn up and circulated by the inspection team enables the service to prepare in advance. This is the standard procedure when the commission wishes the intelligence service to give a presentation on a specific

topic, or when the oversight visit focuses on specific cases. However, the specific targets of data and traceability controls, on the one hand, and controls of operational authorisations granted for international surveillance, on the other, are not announced in advance. This ensures that these inspections are conducted under conditions that are as realistic and genuine as possible.

The law grants the commission the right to access the data necessary for its oversight. It requires ministers, public authorities and public officials to take the necessary measures to facilitate its work, and it penalises any act that might obstruct such work[37].

In this context, the commission has, from the outset, considered that its oversight must respect the adversarial principle. In return for the essential transparency expected of the intelligence services, the findings made by the Commission during its oversight must be subject to the right to be heard and to respond.

This principle is embodied first and foremost during the review, which is a time for dialogue. This dialogue enables the service to explain the aims and reasons for its investigations in greater detail than was possible in the written correspondence when the request to deploy an intelligence-gathering technique was made. Conversely, it gives the commission's representatives the opportunity to understand the functioning of the service, or to draw connections between various elements that had previously been examined in isolation, even though they require a broader perspective. It is not uncommon for such dialogue to lead the commission to explain its position, or even to conclude that its position needs to be supplemented or amended.

The adversarial principle also characterises the follow-up to on-site inspections. Where, at the conclusion of an inspection, the commission observes a discrepancy between its findings and the legal framework,

37. Art. L. 833-3.

it notifies the intelligence service concerned of an anomaly. This report then calls for a response from the service and, where necessary, an exchange of views where the service does not agree with the commission's findings or where the commission is not satisfied with the service's response. This process ensures the necessary understanding between the intelligence services and the commission and, once the findings are agreed upon, progress in ensuring compliance with the legal framework.

VISITS TO THE OPERATIONS CENTRES OF THE INTERMINISTERIAL CONTROL GROUP (GIC)

Each year, the commission undertakes around ten visits outside the headquarters of the intelligence services. It visits the GIC's operations centres, which are spread across mainland France and overseas territories. These centres enable officers from the services in their remit to review the results of the intelligence-gathering techniques that the GIC is responsible for implementing, such as security interceptions.

During these visits, the commission meets with all the intelligence services operating in the region. These direct exchanges, which are of great interest, help to foster mutual understanding. For the commission, this provides an opportunity to gain a more detailed understanding of regional specificities and the threat situation at local level, and to assess the liaison between regional bodies and their central management. For the services, it provides an opportunity to shed light on certain aspects of the legal framework or the opinions issued by the committee.

In 2025, as in previous years, the committee held discussions with the prefectural and judicial authorities during some of these visits, in order to gain a better understanding of the threats and to assess the operational coordination between administrative policing and criminal investigation.

2.2. 120 *ex post* controls carried out in 2025

2.2.1. | Trend in the number of controls over time

In 2023, an increase in its staff numbers enabled the CNCTR to carry out 136 inspections. In 2024, within the context of the organisation of the Olympic and Paralympic Games, the CNCTR managed to carry out 123 inspections. In 2025, the commission met the target of 120 inspections set for it by the legislature, without exceeding it.

This situation can be explained in particular by the growing number of requests submitted for *ex ante* scrutiny, which, with staffing levels remaining constant[38], limits the resources the commission can devote to *ex post* scrutiny, but also by the ever-increasing volume of data -often of a heterogeneous nature- to be scrutinised, due in particular to the growth of the RDI.

2.2.2. | Two significant advances, achieved with the assistance of the intelligence services

The commission must continually adapt the procedures for its *ex post* oversight activities so that they keep pace with developments in the work of the intelligence services.

Two significant advances were accomplished in 2025. One is methodological in nature and the other is technical. These were made possible by the effective cooperation of two first-circle services. The CNCTR wishes to commend these advances.

38. See Part 3, p. 71.

Whilst the law does not provide for any '*immediate*' access[39] to the data collected through the collection and recording of computer data technique, with the result that the commission must visit the relevant intelligence service to access such data, in 2025 a first-circle service agreed, on a trial basis, to forward to the commission, for oversight purposes, certain intelligence reports resulting from the use of the RDI technique.

The commission draws a positive conclusion from this trial. Remote access to intelligence reports resulting from the RDI enables a more thorough qualitative review of an intrusive technique, which is more difficult to assess within the service itself due to the technical constraints inherent in IT tools and the need to keep the on-site inspection within a reasonable timeframe. However, the benefits of such remote access are diminished when surveillance involves other intelligence-gathering techniques that can only be reviewed on-site.

The commission also emphasises the need, both for the service and for itself, to preserve the adversarial nature of the oversight, even if the review takes place remotely rather than on-site.

We should therefore capitalise on the benefits of this significant step forward, whilst working with the intelligence service to find ways of overcoming the limitations identified.

However promising this trial may be, it cannot, on its own, be sufficient. Methodologically speaking, it is merely a precursor to the centralisation at the GIC of all RDI[40] outputs, which was decided in 2023 and is due to be completed by mid-2027. The project is currently underway, under the project management of the National Intelligence and Counter-Terrorism Coordination and the General Secretariat for Defence

39. Article L. 833-2 thus provides that: *'In order to carry out its duties, the Commission shall: [...] 2° Shall have permanent, full and direct access to the records, registers, information collected, transcripts, extracts and transmissions referred to in this Book, to the systems for tracing the information collected and to the premises where such information is centralised pursuant to Article L. 822-1, as well as to the information referred to in Section III of Article L. 822-2'*. Article L. 822-1, for its part, provides that: *'The Prime Minister shall organise the traceability of the implementation of techniques authorised under Chapter I of this Title and shall lay down the procedures for centralising the information collected.'*
To this end, a record is drawn up of each instance in which an intelligence-gathering technique is employed. It sets out the start and end dates of such use, as well as the nature of the intelligence gathered. This record is made available to the commossion, which may access it at any time, in full and directly, regardless of its stage of completion.'

40. See the 2024 activity report, pages 19 and 20.

and National Security. It involves the GIC and the two largest agencies within the first circle.

The second development is of a technical nature. It was achieved with the assistance of the Directorate-General for External Security. This department has enabled CNCTR team members to learn how to use the data processing and analysis tools employed by its own officers. This is particularly crucial when dealing with large volumes of data, as is the case, for example, with international surveillance operations.

As a result, the commission's investigations are faster and more targeted. This makes it possible to focus discussions with the relevant departments on more reliable assessments and to carry out a more comprehensive legal analysis.

This joint initiative is all the more important in the commission's view that the technical aspects of public intelligence policy represent a challenge for it. The commission's size and resources are modest and bear no comparison with those of the intelligence services. This natural difference must not be allowed to develop into such an imbalance that the commission is no longer able to understand how the intelligence services actually use the data collected and is therefore no longer able to exercise effective oversight.

Building on such progress and seeking the most effective controls methods, the commission intends to move forward in 2026. In particular, it wishes to offer certain departments, at regular intervals, 'review controls' focused not on gathering new findings but on analysing the main irregularities already detected, in order to ensure they are resolved more effectively.

These advances and strategic directions help to bridge the growing gap between the requirements of the CNCTR's remit and the resources made available to it, against a backdrop of an increasing number of anomalies being detected.

2.3. Anomalies detected

The number of anomalies detected rose significantly in 2025. This increase is primarily due, on the one hand, to more targeted inspections carried out by the CNCTR and, on the other hand, to the growing effectiveness of inspection techniques, particularly in the field of international surveillance.

The number of anomalies identified in each agency cannot be disclosed without breaching national defence secrecy. The commission further emphasises that this would not constitute a meaningful or sufficient indicator of the legality of the intelligence services' actions. Indeed, on the one hand, not all irregularities are of equal significance. On the other hand, although the commission's oversight work focuses on what it considers to be the most significant legal risks or the most worrying uncertainties, it is not exhaustive.

In essence, the rationale behind the commission's oversight is to ensure the legality of the intelligence services' actions, in all aspects of their work. It is not within the remit or powers of the CNCTR to rule on the appropriateness of the services' actions or on the effectiveness of those actions. This oversight is fundamentally the responsibility of the Government, assisted by the National Intelligence and Counter-Terrorism Coordination, and of Parliament. The dialogue between the commission and the intelligence services sometimes leads the latter to argue before the commission that it should not interfere in operational matters.

Whilst this is beyond dispute when it comes to decisions to act or not to act, for the reasons set out above, it is not uncommon for legal analysis to intersect with considerations of appropriateness: the link between a person under surveillance and the purpose for which they should be monitored, the extension of surveillance which has,

to date, failed to substantiate the intelligence service's assumptions are examples of this intersection. Similarly, the legal review of proportionality requires that the commission be able to assess the relationship between the circumstances of the threat and the measures implemented to prevent it.

A telling example of this debate is the distinction between administrative policing and judicial action.

The Constitutional Council emphasised the importance of this in its decision of 23 July 2015 on the Intelligence Act. Having drawn upon the provisions of Article 16 of the Declaration of the Rights of Man and of the Citizen concerning the separation of powers, it reiterated that 'the gathering of intelligence (…) may have no other purpose than to preserve public order and prevent offences; (…) it may not be used to establish breaches of criminal law, to gather evidence of such breaches or to identify the perpetrators'[41].

Consequently, surveillance cannot continue within the framework permitted by the Internal Security Code once it has yielded sufficient material evidence to establish an offence or a crime. The matter then falls within the remit of the judicial authorities, to whom it must be referred.

Admittedly, the evidence is rarely complete or clear-cut, and the commission readily acknowledges that the intelligence service has a margin of discretion regarding the point at which the matter transitions from administrative policing to judicial action. It emphasises, however, that this discretion, far from being based solely on operational considerations, has a legal dimension of a constitutional nature, and the commission must ensure that this is respected.

As in previous years, anomalies relate to data collection. These may concern the scope or duration of the authorisation and, more rarely,

41. Decision No. 2015-713 DC of 23 July 2015, *paras.* 5 and 9.

the person concerned. In particular, the commission notes once again that certain restrictions set out in its opinions – and taken into account by the Prime Minister when granting authorisation – are subsequently not complied with. The recurrence of this situation raises questions and calls for greater clarity in the authorisations granted to the relevant agencies.

The commission is pleased to note that, in 2025, there has been an improvement in the agencies' traceability practices, an area in which irregularities were previously all too common[42]. Effective traceability is the primary prerequisite for compliance with fundamental legal requirements concerning the conditions for implementing an intelligence-gathering technique or the time limits for data retention. It must be immediate and not provided long after the operation has taken place; it must be accurate, precise and tamper-proof[43]. As they had undertaken to do, these services have improved their practices. These efforts must continue in 2026.

The commission notes, however, that anomalies relating to data retention and use have persisted for the past ten years. It therefore encourages intelligence services to exercise rigour and vigilance when drawing up traceability records, applying the legal provisions relating to data retention periods, and compiling information reports.

The commission reiterates that the external and independent monitoring role entrusted to it complements, but does not replace, the internal monitoring role that each service is required to carry out.

In the area of international surveillance, the CNCTR has identified a higher number of anomalies compared with previous years. This trend does not indicate an increase in errors on the part of the intelligence services, but rather the commission's enhanced investigative capacity, which has enabled it, in collaboration with these services, to develop

42. See the CNCTR's 9th activity report for 2024, p. 76.
43. *Ibid.*, p. 80.

more effective oversight tools. It is now necessary to work with the intelligence services to ensure better compliance with the legal framework governing international surveillance.

Finally, the commission regrets the occasional but recurring difficulties which its inspection teams come up against in accessing certain intelligence services, whether in terms of physical access (e.g. access badges, security clearances) or IT access (computers, printers, etc.). When they arise, these logistical and practical difficulties significantly undermine the effectiveness of the inspections. The commission expects the services concerned to take proactive measures.

2.4. 105 complaints in 2025

This represents an increase of more than 20 per cent compared with the previous year.

2.4.1. | Reminder of the legal framework

In its decision of 10 December 2024, the European Court of Human Rights (ECHR) recognised the decisive role played by the intervention of the CNCTR and subsequently by the specialised chamber of the Council of State in ensuring the effectiveness of the right to a remedy in relation to intelligence-gathering techniques and the fairness of the rules of procedure[44].

Any person may refer a matter to the CNCTR if they wish to verify that no intelligence-gathering techniques are being, or have been, unlawfully used against them. This preliminary complaint procedure is provided

44. ECHR, Fifth Section, 10 December 2024, Association Confraternelle de la Presse Judiciaire and Others v. France, No. 49526/15.
See the CNCTR's 9th activity report for 2024, Part 3, pages 97 et seq.

for under the provisions of Article L. 833-4 of the CSI in respect of so-called 'domestic' techniques and under those of Article L. 854-9 in respect of the surveillance of international electronic communications.

The powers of scrutiny conferred on the commission relate solely to the intelligence-gathering techniques provided for by the CSI. They therefore do not extend to surveillance measures ordered by the judicial authorities, nor to surveillance carried out by the intelligence services using means other than intelligence-gathering techniques, nor to any surveillance – which in any case is illegal – that might be carried out by private individuals.

In practice, for reasons of national security and pursuant to the provisions of Decree No. 2015-1405 of 5 November 2015 concerning exceptions to the right of users to submit applications to the administration electronically, individuals who wish to have checks carried out concerning them may only validly submit a request to the commission by letter sent by post.

The complaint must be submitted by the person concerned or their legal representative, must specify the technical identifiers on the basis of which they wish the checks to be carried out, and must be accompanied by the relevant supporting documents.

The law does not permit the commission to disclose to the individual whether or not they are under surveillance, as this would amount to revealing a protected secret. Pursuant to the provisions of Article L. 833-4, the commission therefore notifies the complainant '*that the necessary checks have been carried out, without confirming or denying that they have been under surveillance*'.

A case may be brought before the Council of State under Article L. 841-1 by any person who can demonstrate that they have previously exercised their right to lodge a complaint with the CNCTR.

The CNCTR is notified of any application lodged on this basis and is invited to submit written or oral observations. It thus has observer status before the Council of State. As the decision-making authority, the Prime Minister, represented by the GIC, is authorised to defend the case on behalf of the State.

2.4.2.| Trends in the number of complaints

The number of complaints has been rising for the past five years. Year 2023 saw a significant increase of more than 65 per cent. In 2024, the number of complaints rose by 7.5 per cent only. In 2025, the rate of increase accelerated again, with a rise of more than 20 per cent. For the first time, the 100-complaint threshold was exceeded in 2025. This means the commission has to investigate approximately one complaint every three days.

	2021	2022	2023	2024	2025	2024/2025 Change	2021/2025 Change
Number of complaints	**48**	**49**	**81**	**87**	**105**	**+20.7%**	**+214%**

2.4.3.| Average time taken to process complaints

The processing time has increased for the third consecutive year, but remains satisfactory:

	2023	2024	2025
Average time taken to process complaints (in days)	**19**	**25**	**27**

In 2025, the average time taken to process complaints was 27 days. This remains below the 45-day target set by the legislature in the annual performance plan annexed to the Finance Act, but it has increased: it was 19 days in 2023 and 25 days in 2024.

The modest nature of this increase and the commission's ability to respond within a reasonable timeframe are mainly due to the nature of the complaints, which rarely involve lengthy or complex investigations.

If the rise in the number of complaints were to continue in 2026, the commission expects, given the resources allocated to it, that the average processing time will continue to deteriorate.

Finally, the commission reiterates here the observation it had already made in its 2023 activity report regarding the absence of any time limit on the complaints it receives and the investigations it is required to carry out[45]. The provisions of the CSI do not provide for any time limit. Unless otherwise specified by the complainant, each complaint is therefore deemed to cover the entire period since the entry into force of the Intelligence Act of 24 July 2015. This lack of a time limit becomes a slightly greater burden with each passing year. Whilst it does not meet any fundamental legal requirement, it is likely to pose increasing difficulties for both the services and the commission in terms of data retention and the conduct of investigations. It would be appropriate to undertake a legal review of this issue and to resolve the current ambiguity in whatever manner the legislator deems appropriate.

2.5. The number of appeals brought before the Council of State remains very low

In 2025, the CNCTR submitted observations on the nine applications referred to it by the Council of State.

45. See 2023 Activity Report, pp. 87 and 88.

Part 3. Overview, challenges and perspective

3.1. An outward-looking approach

Despite the demands of its supervisory role[46], the commission has continued to develop its work with its various partners.

Throughout 2025, the commission held regular discussions with Parliament. In particular, it appeared before the relevant committee of the National Assembly on the draft law on drug trafficking[47] and before the special rapporteur for the draft law known as 'Resilience' bill[48]. The commission also presented its 2024 activity report to the Speakers of both Houses, the Parliamentary Intelligence Committee, and the Legal Affairs and Defence Committees of both the National Assembly and the Senate. On these occasions, it was able to reflect on its prospects for future development, ten years after its creation. The CNCTR emphasises the importance it attaches to Parliament's attention to all matters relating to public intelligence policy.

On 22 September 2025, the commission held a special symposium to mark its tenth anniversary, with the aim of taking stock of its work and putting the simple yet fundamental question: whether it was fulfilling its remit adequately, to the general public. The exchange of views between parliamentarians, intelligence officials, academics, senior civil servants and journalists helped to answer this question. The proceedings from this symposium[49] are published in the CNCTR's tenth-anniversary compendium, which is being published at the same time as this activity report.

46. See Parts 1 and 2.
47. Bill aimed at freeing France from the trap of drug trafficking, Act No. 2025-532 of 13 June 2025.
48. Draft Bill on the resilience of critical infrastructure and the strengthening of cybersecurity, No. 1779.
49. See the 10-year anniversary compendium on the CNCTR website under the 'Our Events' section. In French only.

On 5 and 6 November 2025, the commission took part to the European Conference on Intelligence Oversight in Zurich, at the invitation of the Swiss intelligence oversight body. This conference brings together, on a regular and informal basis, the national intelligence oversight authorities from numerous European countries and Canada.

The structure of these authorities varies according to the institutional and legal traditions of each country. Some authorities are administrative in nature and very similar to the CNCTR, whilst others are parliamentary or judicial in nature. Several countries divide the role between several separate oversight bodies.

Beyond those differences, such exchanges provide the commission with an opportunity to strengthen its ties with its counterparts, to discuss with them the legal, institutional and operational aspects of effective and responsible intelligence oversight, and also to address the challenges that oversight bodies may face.

Finally, the commission has pursued its dialogue with the academic community. It attaches great importance to such exchanges as they contribute to the recognition of intelligence law as a branch of law in its own right and promote understanding and analysis of the French legal framework by researchers, lecturers and students.

It has contributed to the initial and continuing training of intelligence service staff and managers during sessions organised by the Intelligence Academy, which operates under the authority of the Prime Minister and is a member of the French intelligence community. It has taken part in some ten such events in 2025. These events enable the commission to raise awareness of its work and to respond directly to questions from front-line staff and managers attending these training sessions.

In the same vein, members of the commission's board took part in several continuing professional development sessions organised by the National School for the Judiciary. Given, on the one hand, that it is not uncommon

for an administrative police investigation to precede referral to the judicial authorities and, on the other hand, that criminal investigations may employ the same techniques but within a different legal framework, these exchanges are of great importance to the Commission.

3.2. Unchanged resources

In 2025, the commission carried out its tasks with a stable workforce.

Staff members are the commission's greatest asset. It has 22 staff members, including 14 legal and technical officers, and 9 members of the board. Of the latter, four are Members of Parliament whom take part in the commission's plenary deliberations. The day-to-day work is effectively carried out by the five permanent members, four of whom work full-time.

In 2025, the commission underwent numerous changes: its chairman, its board member appointed for his technical expertise, its secretary-general, and nearly a third of its legal and technical officers.

The diversity of the professional backgrounds and cultures of the commission's staff[50] is essential to maintaining the multidisciplinary approach required by the scope of its remit and the variety of services it is tasked with scrutinising.

It now appears essential to strengthen the commission's resources, given the upward trend in the number of applications: a 50 per cent increase since 2016 and a 15 per cent increase since 2021; the growing complexity of the technical matters which the commission must analyse in depth in order to deliver a truly informed opinion on the compatibility

50. Judicial and administrative magistrates, scientific and technical staff, police superintendent, senior gendarmerie officers, armaments engineers, customs officers, analysts.

with the legal framework; and the current lack of a comprehensive solution for remote *ex-post* inspection that would improve efficiency.

The limited human resources (jobs and total wage bill) allocated in 2025 place the commission in a difficult position.

A repeat of this situation in 2026 poses a critical risk to its ability to fulfil the mission entrusted to it. The resources allocated to the main intelligence services have increased significantly in recent years. This increase is justified by the need to protect the Nation, going beyond the scope of public intelligence policy alone. The CNCTR is, of course, not suggesting that its own resources should be indexed to this growth; rather, it draws attention to a real risk of falling behind.

The commission's resources in 2024 and 2025		
	2024	2025
Number of staff	22	22
Job creation authorised by the legislature ('Employment Plan')	+2*	0
Number of members of the board	9	9
	Of whom 4 are full-time	Of whom 4 are full-time
Total payroll	3,035,601	3,151,262

** Creation of two posts in support functions, notably the information system, which was developed and managed by a single staff member until 2023.*

3.3. The CNCTR highlights the fact that two issues remain unresolved: the lack of a regulatory framework governing exchanges between French and foreign intelligence services, and the issue of 'sovereignty files'

3.3.1. The lack of a regulatory framework governing exchanges between French and foreign intelligence services

In its Grand Chamber judgment in *Big Brother Watch and Others v. the United Kingdom and Centrum för rättvisa v. Sweden* of 25 May 2021, the European Court of Human Rights (ECHR) accepted the justification for data-sharing between the intelligence services of several countries but held that, unless the protection afforded by the European Convention were to be rendered meaningless, such exchanges must be subject to a regulatory framework and supervised by an independent authority capable of monitoring them. The Court found that, in this particular case, the framework governing exchanges between the UK intelligence services and the *National Security Agency* of the United States of America was satisfactory.

The CNCTR has on several occasions, both before and after this decision, emphasised the need for the French Government and legislature to draw the necessary conclusions from this decision[51]. In the absence of any progress, it therefore reiterates this call.

It emphasises that not only does our positive law fails to provide any regulatory framework, but it also doubly precludes the possibility of monitoring such exchanges.

51. See the 2018 activity report, p. 50 et seq., the 2021 activity report, p. 50 et seq., the 2022 activity report, p. 69 et seq., the 2023 activity report, p. 80 et seq., and the 2024 activity report, p. 100.

On the one hand, the provisions of Article L. 833-2 of the CSI relating to the CNCTR's remit stipulate that it may '*request from the Prime Minister all information necessary for the fulfilment of its remit (…) with the exception of information provided by foreign services or international organisations (…)*'. On the other hand, the matter is largely exempt from parliamentary scrutiny since, under the terms of Article 6 *nonies* of Order No. 58-1100 of 17 November 1958 on the functioning of parliamentary assemblies and establishing the Parliamentary Intelligence Committee, the latter '*(…) may, within the limits of its need-to-know, request the Prime Minister to provide (…) any other document, information or assessment necessary for the fulfilment of its remit. / Such documents, information and assessments may not relate (…) to exchanges with foreign intelligence services or with international organisations competent in the field of intelligence*'.

Exchanges between French and foreign intelligence services are legitimate and necessary for the protection of the Nation's fundamental interests. The aim of regulating such exchanges must be to meet the clear requirement set out by the ECHR, not to call them into question or to hinder them.

Whilst it is not for the commission to prescribe the details of such a legal and regulatory framework, it could be in line with the following principles and requirements:

- The principle of reciprocity, as is customary in matters of international administrative assistance;
- With regard to information provided by the French authorities, on the one hand, the principle that the law of the receiving State authorises it to collect information of a similar nature in comparable circumstances and, on the other hand, the requirement that the receiving State provide sufficient safeguards regarding the use, retention and non-disclosure of the data;

- With regard to information received by French authorities from their foreign partners, the symmetrical principle requires that French law permit the collection of information of a similar nature in comparable circumstances.

The CNCTR's supervisory remit should be extended to cover the transmission of information gathered by the French authorities pursuant to Book VIII of the CSI, and the receipt of such information by foreign partners where it is of a similar nature. The supervisory role of an independent authority, as defined above, could be adapted depending on whether or not the partner State is a party to the European Convention for the Protection of Human Rights and Fundamental Freedoms.

3.3.2. The issue of 'sovereignty files'

Article L. 841-2 of the CSI provides that the Council of State has jurisdiction to hear applications concerning the implementation of the Act of 6 January 1978 'Data Protection Act' in relation to data processing affecting national security; Article R. 841-2 sets out the list of such processing operations.

However, it is not certain that these provisions provide a precise definition and list of what the intelligence services refer to as 'sovereignty files'.

These files may contain, in addition to data derived from intelligence-gathering techniques, data from other sources, including foreign intelligence services, or data that may reveal the identity of the service's sources, or analyses specific to the service. The French intelligence services conclude that the CNCTR's oversight cannot extend to these files.

As with the previous question, the commission has repeatedly highlighted the difficulties arising from this position[52].

52. See, in particular, the 2019 activity report, p. 75, the 2020 activity report, p. 74, the 2022 activity report, p. 71, the 2023 activity report, p. 80.

These difficulties do not relate to matters which the law does not task the commission to scrutinise. Article L. 833-2, as already mentioned, excludes, for example, the commission from considering matters which might reveal the identity of a source. Nor is the commission tasked with assessing the strategy of the intelligence services or the effectiveness of their operations; it therefore has no intention of extending its scrutiny to analyses or summaries setting out such operations.

The commission merely points out that data collected in accordance with the provisions of Book VIII of the CSI must comply with those provisions, wherever they are stored. It must therefore be able to access them. It adds that the mere name of a file or folder is not sufficient to determine or guarantee its contents. Such a name is therefore not, in itself, sufficient to deprive the commission of the legal right of access to which it is entitled.

The CNCTR is convinced that it is possible to develop the legal and technical arrangements needed to reconcile the requirements for such access with the limits placed upon it. Building on the trust established between the intelligence services and itself, it calls on them, as well as the National Coordination Body for of Intelligence and Counter-Terrorism , to undertake this work.

3.4. Among the areas requiring vigilance, algorithms and cryptanalysis occupy a prominent place

Two important issues relating to intelligence law characterised 2025 and will remain relevant in 2026: the aims and content of what is known as 'algorithmic techniques', on the one hand, and the issue of the encryption of communications, on the other.

3.4.1. Algorithm: a missed opportunity in 2025, which offers a chance for greater security and clarity

Article L. 851-3 of the Internal Security Code establishes the intelligence-gathering technique known as the 'algorithm', which enables the detection of weak signals that may indicate a threat. Once the anonymity surrounding such a signal has been lifted, surveillance based on other intelligence-gathering techniques may confirm or rule out the risk.

The commission refers to the study it devoted to this technique in its 2024 activity report: 'The algorithm within the meaning of the Internal Security Code: from a fantastical vision to a legal reality'.

Algorithm may only be used by specialised intelligence services. Like any other technique, it must serve the purpose for which it is intended, as strictly defined by Article L. 811-3. To ensure this link, it relies on data derived from communications networks which may reflect the behaviour of a person posing a risk or a threat in relation to that purpose.

Introduced by the 2015 Act to detect links that might reveal terrorist threats[53], the technique was extended to the prevention of foreign interference (purpose 2) or threats to national defence (purpose 1) by Act No. 2024-850 of 25 July 2024 aimed at preventing foreign interference in France.

Article 15 of the Act aimed at freeing France from the trap of drug trafficking, which originated from a Senate bill, provided, in the version finally adopted by Parliament on 29 April 2025, for the extension of the use of the algorithmic technique to purpose 6, in order to enable the detection of threats arising from certain forms of organised crime and delinquency

53. A measure originally introduced on an experimental basis under Article 25 of Act No. 2015-912 of 24 July 2015 on intelligence, extended on two occasions by Article 17 of Act No. 2017-1510 of 30 October 2017 strengthening internal security and the fight against terrorism, and subsequently, in the context of the Covid-19 pandemic, by Act No. 2020-1671 of 24 December 2020 on the extension of Chapters VI to X of Title II of Book II and of Article L. 851-3 of the Internal Security Code, and subsequently made permanent by Article 15 of Act No. 2021-998 of 30 July 2021 on the prevention of acts of terrorism and on intelligence.

(drug trafficking, trafficking in arms and explosives, and the laundering of the proceeds thereof[54]). The provision adopted retained the wording that the commission, to which the Prime Minister had referred a draft amendment to the provisions of Article 8 of the bill, had proposed in its deliberation No. 1/2025 of 13 March 2025[55].

These provisions were referred to the Constitutional Council. Before reaching a decision, it heard evidence from the Chairman of the CNCTR. In its Decision No. 2025-885 DC of 12 June 2025, it ruled that extending the use of the algorithm to purpose 6 served the constitutionally protected objectives of safeguarding public order and preventing offences (*para*. 122). However, having been asked in the referral to rule on the provisions introduced in 2021 relating to the use in algorithms of the full addresses of internet resources, or URLs[56], it ruled that such use was not accompanied by sufficient safeguards to ensure a balanced reconciliation between the constitutionally protected objectives of safeguarding public order and preventing offences and the right to privacy (*para*. 127 and 128). It therefore ruled that both the 2021 provisions authorising the use of URLs[57] and those of the referred Act extending the use of algorithms to purpose 6 were contrary to the Constitution. This extension is deemed unconstitutional solely on the grounds of the absence of safeguards surrounding the use of URLs.

When consulted in 2021 on the draft bill including URLs amongst the data that could be used by algorithms, the commission had considered this inclusion to be possible. It had, however, emphasised, as it had previously in 2016[58], the specific nature of URLs, which are connection data within the meaning of Article L. 851-1, but which may also contain data relating to the content of the correspondence exchanged[59].

54. More specifically, the bill targeted 'threats relating to organised crime and organised delinquency concerning offences punishable by ten years' imprisonment, insofar as they relate to the trafficking of narcotics, arms and explosives trafficking, the import and export of these prohibited goods committed by an organised gang, and the laundering of the proceeds thereof'.
55. Available on the Commission's website: cnctr.fr.
56. *Uniform Resource Locator*.
57. Article 15 of Law No. 2021-998 of 30 July 2021, referred to *above*.
58. Decision No. 1/2016 of 14 January 2016, available on the cnctr.fr website.
59. Decision No. 2/2021 of 7 April 2021, in particular pages 4 to 7.

CONNECTION DATA, DATA RELATING TO THE CONTENT OF COMMUNICATIONS, URLS: WHAT ARE THEY?

Connection data refers to the technical data that enabled the transmission of an electronic communication, of which it constitutes a record. It forms a 'container' which, in principle, provides no indication of the 'content' exchanged. It is, however, sensitive in nature in that it may reveal details about a person's private life, such as daily routines, places of residence or movements.

A URL is a string of alphanumeric characters that points to digital 'locations' and thus enables communications to be routed. In this respect, it constitutes connection data.

However, a URL may also contain information about the content being accessed[60]. For example, the URL *https://www.dunod.com/sciences-techniques/equations-differentielles-cours-et-exercices-corriges* reveals information about the content of the page it provides access to: lectures and exercises relating to differential equations.

URLs thus combine connection data and content data.

The Constitutional Council did, admittedly, note the safeguards provided by the CNCTR's oversight of the algorithm's technical aspects (*considerations* 125 and 126). However, drawing on the dual nature of URLs and the impact that what URLs reveal has on privacy, it ruled that their use in an algorithm should be subject to conditions '*relating in particular to the nature of the data revealed by the full addresses of resources used on the internet*'.

The CNCTR is convinced that a balance between the right to privacy and the purpose of safeguarding public order and preventing offences can, in this area, be achieved.

60. CNIL Decision No. 2015-455 of 17 December 2015.

The draft bill updating the military planning for the years 2024 to 2030, adopted by the Council of Ministers on 8 April 2026 and tabled on the same day in the National Assembly, contains, in Article 18, provisions designed to address the implications of the Constitutional Council's decision. In addition to reintroducing the extension of the technique to purpose 6, the draft text specifies and describes the categories of URLs that may be used in an algorithm and strengthens the provisions relating to consultation with the CNCTR on any proposed algorithm. The commission considers that these provisions are such as to meet the constitutional requirements.

The commission considers this safeguard to be important and reiterates its commitment to closely examining and monitoring the technical aspects of Article L. 851-3 at every stage.

Firstly, the review of a proposed algorithm –which precedes the commission's opinion and the Prime Minister's authorisation– must convince the commission's panel that the threat in question and the difficulty in identifying the individuals posing that threat justify the use of an algorithm. The same applies to the weak signals to be detected and their sufficiently direct link to the intended purpose. The settings of the parameters implemented to meet these objectives must comply with the principle of proportionality: they must not generate an excessive number of signals. The daily review of requests to lift anonymity on signals generated by an algorithm enables the commission to monitor variations in these signals.

Secondly, the same requirements and analyses are applied to any substantial request to modify an algorithm: such a modification is treated in the same way as an initial request.

Thirdly, the commission must, with the assistance of the GIC – which is legally the sole operator of an algorithm – be able to control its operation, right down to the details of the computer code.

Fourthly, and as provided for by law, any application for the renewal of an algorithm must include an analysis of the relevance of the alerts generated, so that the justification and proportionality of the technique can be assessed on an ongoing and frequent basis[61].

The debate on this bill must also provide clarification.

Firstly, the Constitutional Council's ruling highlighted the need for the law – if it is to permit the use of URLs through this intelligence-gathering technique – to explicitly set out the safeguards and limitations on such use. The committee would have ensured that such safeguards were in place had it been called upon, from 2021 onwards, to rule on a draft algorithm utilising URLs; their express mention in the law will strengthen the framework. Secondly, national defence secrecy precludes any precise description of the purpose and functioning of existing or future algorithms. This constraint frustrates the public's legitimate expectations and hinders any explanation of what this technique is and is not. However, the CNCTR considers that an algorithm, within the meaning of French law, is the opposite of mass surveillance and that the balance between protecting the Nation's fundamental interests and protecting privacy is better guaranteed by an algorithm than by other, less discriminatory and less controlled means.

3.4.2. Communications encryption: a step forward for the right to privacy, a challenge for intelligence services in a democratic state

In a democratic state, the implementation of covert surveillance measures to protect the Nation's fundamental interests must be balanced against respect for citizens' right to privacy.

61. The initial authorisation to operate an algorithm is granted for a maximum period of two months. Renewal may be authorised for a period of up to four months.

This balance is particularly delicate when it comes to the surveillance of encrypted communications. As the European Court of Human Rights (ECHR) has noted, encryption protects the right to privacy but can be exploited by criminals, thereby hindering investigations (ECHR, Section 3, 13 February 2024, Podchasov v. Russia, No. 33696/19, §§ 76 and 78).

However, whilst security interception measures in principle allow access to the content of communications, the situation is different when those communications are encrypted.

Consequently, the increasingly widespread use of encrypted messaging services has significantly reduced the value of security interceptions and led to a growing reliance on the collection and recording of computer data (RDI), as outlined in Part 1 of this report. Indeed, this technique allows access to data on the device without the encryption preventing it from being read. It is, however, particularly intrusive and complex to implement.

The current situation is therefore unsatisfactory. Whilst there is no valid reason why, when surveillance is justified, information relevant to the protection of the Nation's fundamental interests should be overlooked simply because it is encrypted, there is a real risk that a decryption capability could undermine the protection that benefits everyone.

It was against this backdrop that, in 2025, Parliament considered two opposing options in turn.

The first involved requiring providers of encrypted messaging services to grant access to encrypted content. In early 2025, during the public debate on the bill aimed at freeing France from the trap of drug trafficking, the Senate introduced Article *8ter*[62] amending Article L. 871-1 of the CSI to replace the obligation –deemed impractical– on encrypted messaging operators to provide '*arrangements enabling the decryption*

62. Amendment No. 73 rect. ter of 28 January 2025.

of data' —whilst immediately offering the possibility of exemption '*if they demonstrate that they are unable to comply with such requests*'— with the obligation to implement, without exception, '*the technical measures necessary to enable access to intelligible content*'.

This article was deleted by the National Assembly's Committee on Constitutional Affairs, Legislation and General Administration of the Republic[63], on the grounds that, in its view, it posed a risk of infringing fundamental rights –in particular the right to privacy– in that the measure would allow for the introduction of 'backdoors' that undermine everyone's ability to use encryption, even though it is a means of protecting the right to privacy and the confidentiality of online correspondence.

The second option, by contrast, was to impose a general and absolute ban on the imposition of any obligation such as that envisaged by Article *8ter*, whether relating to encryption or any other mechanism enabling unauthorised access to protected data. Thus, in September 2025, during the scrutiny of the draft bill on the resilience of critical infrastructure and the strengthening of cybersecurity, the Senate introduced[64] an Article *16bis* stipulating that operators of encrypted messaging services could not be required to incorporate measures designed to '*deliberately weaken the security of information systems and electronic communications, such as master decryption keys*'.

Article *16bis* also prohibits '*any other mechanism*[65] *that allows unauthorised access to protected data*'. It should be noted that these provisions make no distinction between investigations conducted as part of administrative policing and those ordered by the judicial authority. It should also be emphasised that, given their wording, they could be interpreted as extending the prohibition they lay down to any data other than that which is encrypted, provided that it is protected.

63. Amendments No. CL44 of 21 February 2025 and Nos. CL176, CL205, CL282, CL312 and CL335 of 28 February 2025.
64. Amendment No. 1 rect. quinquies of 12 March 2025.
65. The National Assembly will add 'or process': amendment CS358 of 5 September 2025.

To date, this provision has not been definitively adopted.

The commission notes that, in both cases, there was little evidence to inform the 2025 debates. It recommends that any proposed reform relating to encryption, whatever its direction, should be based on an in-depth legal analysis, underpinned by the most comprehensive technical expertise possible, and that all these elements should be presented for debate in a comprehensive impact assessment.

In any event, any such proposal must be compatible with the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Article 8 of this Convention stipulates that '*everyone has the right to respect for his private and family life (…)*', his home and his correspondence. Paragraph 2 of the same article, however, allows public authorities to interfere with the exercise of this right '*as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety (…), for the prevention of disorder or crime (…)*'.

Where covert surveillance measures intended to protect national security are at issue, the European Court of Human Rights recognises that national authorities have a certain margin of appreciation in choosing the means appropriate to achieve '*the legitimate aim of protecting national security*' (ECHR, Grand Chamber, 4 December 2015, Roman Zakharov v. Russia, No. 47143/06, para. 232).

However, the court checks, on the one hand, that the measure is '*provided for by law*' –that is to say, accessible and foreseeable– and, on the other hand, that this measure is '*necessary in a democratic society*', which presupposes the existence of '*adequate and effective guarantees against abuse*' (*Ibid.*), assessed in the light of the circumstances of the case (the nature, scope and duration of any measures, the supervisory authority, the type of remedy available, *etc.*).

Applying these general principles, the Court examined the compatibility with Article 8 of the Russian legal provisions requiring telecommunications operators to retain the content of all internet communications, to grant the Russian authorities access to such data upon request and, where necessary, to decrypt the messages (*Podchasov v. Russia*, 13 February 2024, cited above).

Having noted that encryption protects the right to privacy and the confidentiality of online communications, and that it helps to ensure the enjoyment of other fundamental rights such as freedom of expression (*Id.*, § 76), the Court noted that the obligation on operators to decrypt end-to-end encrypted communications necessarily undermines encryption for all users, without distinction, '*including individuals who pose no threat to a legitimate government interest*'. It concluded that this obligation is not proportionate to the purpose pursued (§§ 76–79) and cannot therefore be regarded as necessary in a democracy (*Ibid.*, § 80).

Any future French legislative proposal will have to fall within the framework thus established.

Studies

Study 1. The principle of proportionality

Contribution by Mr. Jean-Marc Sauvé, Honorary Vice-President of the Council of State, former Secretary-General of the Government

The origins of the principle of proportionality

The principle of proportionality is, first and foremost, a matter of common sense. It also has a philosophical dimension that cannot be ignored. And over the past 140 years, this principle has made a spectacular breakthrough in the field of law.

It is, first and foremost, a matter of common sense, which can be summed up as follows – and, as it happens, it is lawyers who are speaking here: '*the police must not use a cannon to shoot sparrows*', Fleiner, 1912. Another example: '*You don't use a sledgehammer to crack a nut if a nutcracker will do*', Lord Diplock, 1983. So much for common sense.

At the heart of the principle of proportionality lie the concepts of measure and harmony. Proportion stems from the idea of relating several elements – which may be more or less in conflict with one another – in the quest for balance. According to Aristotle, it is '*the source of justice, in that justice is a middle ground between extremes which, otherwise, would no longer be in proportion*'; I quote from the Nicomachean Ethics.

Building on these initial findings, the principle of proportionality has now become a benchmark for reviewing administrative action where public interests conflict with fundamental rights and freedoms. Consequently, this principle serves, and must serve, as a guide or guiding principle not only for the review of administrative action, but also for administrative action itself, particularly where fundamental rights and freedoms are at stake.

Proportionality in law is a mechanism for balancing legal principles of equal standing that are simultaneously applicable but contradictory. It must make it possible to reconcile conflicting interests and, in particular, the protection of fundamental human rights and freedoms with the preservation of other legitimate aims, such as the public interest or objectives of constitutional significance, such as the protection of the fundamental interests of the Nation, the prevention of breaches of public order, *and so on*. This principle became a standard for reviewing infringements of fundamental human rights, initially in Germany –and I am referring to the Kreuzberg judgement of 1882– but the German Basic Law of 8 May 1949, following the fall of the Third Reich, also refers to the principle of proportionality. Subsequently, this principle was adopted by the European courts from the 1950s onwards. It took the form of a three-part test, namely the assessment of whether public decisions that infringe fundamental rights or freedoms are appropriate, necessary and proportionate. French courts had long been applying an equivalent test, but they too took the step of adopting the term in the strict sense –that is, by using this terminology– the Constitutional Council doing so in 2008 and the Council of State under my presidency in October 2011. I would like to reassure anyone who might be concerned. The UK Supreme Court has also adopted proportionality review, whereas until 2001 it only reviewed whether a public decision was unreasonable or manifestly unreasonable.

The US courts have even embraced this principle. It is a principle that has become a cornerstone of the rule of law, even though it may be interpreted differently depending on the state and the court. It could be said that Anglo-Saxon courts allow public authorities a fairly wide margin of discretion, whereas continental courts exercise more rigorous scrutiny.

In my view, the proportionality test does not have a 'dark side', in the sense intended by Professor Dubout. When a measure examined through the prism of this principle, what is weighed against fundamental

rights and freedoms are, in each specific situation – and these are no small matter – constitutional values that do not stem from the judge's subjectivity, goodwill, mood or imagination. These objectives are enshrined in the Constitution, which the judge – and, before him, the administrative authority – must take into account. Within this framework, the legality of each decision and, consequently, its legitimacy, depend on this balancing of conflicting interests. The decision under consideration is certainly not treated as absolute by the reviewing body; the reviewing body must maintain a distance from the decision that is proposed or taken. However, this initial decision, which is the subject of the review, is neither viewed with *a priori* suspicion nor regarded as insignificant.

What is truly striking about the history of the review of public action is that, in the 1910s and 1920s, the principle of proportionality was applied to matters as complex –if I may say so by way of antithesis– as the ringing of church bells, religious processions on public roads, the seizure of newspapers, or bans on public meetings. At that time, it was not all that difficult to carry out a relatively well-informed proportionality review. Today, this review applies to the implementation of techniques of a wholly different complexity, which can have consequences that are extremely intrusive and infringe upon freedoms. This is how, on a single foundation, on a single basis, the enduring issue of the proportionality of administrative action arises in radically new terms.

The widespread adoption of the principle of proportionality and the checks on it is by no means a cause for despondency, but is in fact a real source of confidence. It fosters confidence both among citizens and among the officers involved in these operations, because they, too, have a right to safety. With the promotion of the principle of proportionality and the checks on it, one might initially think: 'But we can't do anything anymore. This legal framework is 'of unprecedented complexity'. In reality, I believe that, both from the perspective of safeguarding individual rights and from that of the work of

the intelligence services, such a framework is beneficial. It all ties in because we live in a dangerous world, in which states and groups are prepared to do anything to satisfy either their desire for domination or their criminal enterprises. We must therefore resort to techniques that are extremely sophisticated and intrusive. But because, at the same time, we are a state governed by the rule of law and not a totalitarian or dictatorial state that tramples on freedoms and fundamental rights, we must exercise credible oversight over the use of these techniques.

To ensure that this proportionality review is not perceived as tainted by subjectivity or bias, and that its legitimacy is not challenged, it is important that it be conducted collegially as far as possible, particularly in the case of opinions and decisions of principle. It must also be underpinned by a well-established body of doctrine that is stable and understood by the intelligence services. It is essential that this doctrine is also made public: hence the importance of the CNCTR's public reports, following those of the National Commission for the Oversight of Security Interceptions, so that the work of the oversight bodies is understood by the general public and not just by experts – which, incidentally, remains crucial. For this oversight to be accepted by the bodies being monitored, the oversight body must also take care not to act as a substitute for the services that employ intelligence-gathering techniques.

Everyone has their own role, which is different. From this perspective, a parallel can be drawn with the administration and the administrative court judge. The judge is not an administrator, even though they specialise in reviewing the administration's actions. Dialogue between the supervisory body and the departments is absolutely essential. This has already been highlighted, as I believe that exercising proportionality checks in a highly technical field must truly be carried out with full knowledge of the facts. And so, the departments must report to the supervisor both formally and informally, and then, where appropriate, it is for the judge to determine whether the actions they are taking or intend to take are necessary, appropriate and proportionate. On the other hand, the supervisor has

a pressing duty to educate the departments concerned. This two-way dialogue is absolutely essential.

The principle of proportionality and the technological advancement of surveillance

The threats we face from terrorist or rogue groups or states – particularly in the context of digital technologies – leave little room for manoeuvre for democracies, which are at the same time states governed by the rule of law. It is up to us to defend ourselves, within the framework of the well-known dialectic of the sword and the shield.

If new threats can be tackled by using conventional means, there is no reason to hesitate. But the answer to this question really lies in the proportionality test, which enables us both to assess the response and to determine it. In any case, we must be extremely clear: conventional or traditional methods are, as a general rule, no longer effective in dealing with the threats to which we are exposed. The use of highly sophisticated technologies is therefore, in principle, inevitable. We must therefore assess, on a case-by-case basis, depending on the targets and threats, to what extent they can be used. The collection and retention of connection data enable us to work with vast quantities of data relating to very large populations, even though the number of people we are seeking to identify is often very small and we need to target them specifically. The proportionality test must enable us to weigh up the risks we face against the tools we need to deploy.

The proportionality test is carried out at the level of individual measures and as a preventive measure, but it is also carried out at another level, namely at the stage when the legislation is enacted.

What does the Constitutional Council do when it rules on legislative measures that grant new investigative powers to the intelligence service, if not, in this instance too, exercise a proportionality test? In a number of cases, this is accepted, but in other situations, measures

are struck down. Consequently, the proportionality test is intended to be applied at all levels, both at the legislative level and in relation to individual decisions.

I am a witness to a bygone era. I drafted the letter signed by Prime Minister Pierre Mauroy, more than 40 years ago, asking the First President of the Court of Cassation to examine the issue of telephone tapping. What should be done in this regard? First President Schmelck drew up a report with the support of Bruno Genevois. That report was immediately shelved, and for 10 years nothing happened.

In the meantime, I left the Ministry of Justice and became Director of Civil Liberties at the Home Office. The first memo I wrote to the Minister –whose name I shall not mention– was to tell him: 'Minister, you must introduce legislation on telephone tapping, because the European Commission of Human Rights issued a highly critical opinion this year –the *Kruslin and Huvig* opinion– on the lack of legislation in France regarding telephone tapping, and because a ruling against our country on this matter is inevitable.' My memo was consigned to oblivion, until France was condemned by the European Court of Human Rights on 24 April 1990. I resubmitted my draft bill. As implausible as it may seem, this ruling provoked no reaction and led to no government action. It was a television programme, Jean-Marie Cavada's '*La marche du siècle*', which, in 1991, finally prompted the political class and public opinion to take up this issue, leading to the decision to legislate on it as a matter of urgency – though not without murmurs here and there: 'But what on earth have the intelligence services been doing? They didn't warn us'. I recognise that, in that bygone and now obsolete world, the question of technical expertise did not arise in quite the same terms as it does today: the techniques were simple, and the task was to assess whether the use of intelligence-gathering techniques in relation to specific individuals was proportionate or not. To use a metaphor that I can still grasp, we were, at that time, fishing with a rod and line, rather than trawling. I have realised that, today, fishing

with a rod and line is no longer particularly relevant or effective, and that we now need to operate on a different scale.

Dialogue between the law and technology is absolutely essential. Sound legal decisions cannot be made without a proper understanding of the underlying technical issues. And this applies just as much to intelligence-gathering techniques as it does to all technical disputes –or, for example, medical disputes. Regulators and judges are not there simply to turn a blind eye and rubber-stamp decisions. They must know how to seek out relevant expert opinions or technical assessments and take these into account in order to deliver decisions or opinions that are as well-informed and indisputable as possible. In short, whether one is a legislator, judge or regulator, one must grapple with the technical nature of the issues. We must be fully aware that if, on the grounds of the complexity of the issues, the legislator, judge or supervisory authority fails to fulfil their duties, there will be no oversight whatsoever, with the risk of the abuses we see in countries that are not governed by the rule of law; and then, all of us will have nothing left but our tears. We must be able to defend fundamental freedoms and rights, even when the issues under discussion are complex. And far more complex than any of the issues over which we have clashed in the courts for decades. In the past, the issues were extremely simple and accessible to the man in the street. Today, the questions are framed in very different terms. We must face up to them. Do not think that I am an unconditional supporter of dragnet surveillance. It is simply that there are circumstances of time and place, and threats, which mean that the use of algorithms, the collection and retention of connection data, and other monitoring operations have become indispensable. This represents a major shift from the world of the Cold War 50 years ago.

Study 2. *Ex-post* control as described by those involved

The aim of this study is to provide a practical account of the oversight role carried out by the CNCTR within the intelligence services and to give a voice to everyone involved.

It is based on accounts from both sets of stakeholders: on the one hand, the commission's legal and technical officers and members of its board, who carry out the oversight, and, on the other hand, the teams representing the services subject to oversight during these operations.

The General Directorate for External Security (DGSE), the General Directorate for Internal Security (DGSI) and the National Directorate for Territorial Intelligence (DNRT) have kindly agreed to take part in this exercise. The CNCTR extends its warmest thanks to them.

INTRODUCTION

To ensure comprehensive and effective oversight of the activities of the intelligence services, the legislature has conferred on the CNCTR powers of scrutiny covering all stages of the procedure for implementing intelligence-gathering techniques, from the examination of all applications and the opinion submitted by the Commission to the Prime Minister -who may or may not grant authorisation- to the exercise of *retrospective* oversight over the implementation of the authorisations granted, in order to ensure the proper application of the law.

Broadly speaking, there are four types of oversight:

- Case reviews consist of a joint examination of the surveillance of individual persons or of discussions with the department regarding a phenomenon, an event or a group that warrants surveillance;

- Data checks ensure compliance with the legal requirements for the collection and retention of data in the context of surveillance: traceability of operations, compliance with authorisation periods and retention periods, and the relationship between the information collected and the legal purposes justifying the surveillance;

- Controls relating to international surveillance, as provided for in Articles L. 854-1 et seq. of the Internal Security Code;

- Regional inspections, which enable the commission to liaise -beyond the central headquarters of the intelligence services- with the field units within a defence zone, a region or a department. These inspections take place throughout the country, both in mainland France and in the overseas territories.

The commission carries out these inspections in two ways:

- by visiting the agencies' premises to carry out document-based and on-site inspections, in direct contact with the officers concerned;

- or remotely, from its own premises, using secure IT tools made available to it and to the intelligence services by the Interministerial Control Group (GIC), a body under the authority of the Prime Minister.

In order to carry out its oversight role, the CNCTR has permanent, full and direct access to all information collected, transcribed and extracted during the use of intelligence-gathering techniques, to documents recording these operations, to the systems for tracing such information, and to the premises where it is held.

The CNCTR's review is fundamentally a review of legality. It does not concern either policy considerations or operational decisions of the departments, nor on the effectiveness of their actions. Nevertheless, knowledge and understanding of the context and circumstances are necessary for a proper assessment of compliance with the legal criteria of necessity, proportionality and subsidiarity.

It is based on the principle of adversarial proceedings. The CNCTR places great importance on dialogue with the services and on the educational aspect of its oversight. An control frequently provides an opportunity to clarify misunderstandings regarding the legal framework, to explain the Commission's position, or to share the intelligence services' analysis of difficulties in implementation.

Finally, unlike the *ex ante* review of requests from the intelligence services, which is exhaustive, *ex post* review is necessarily selective. It is for the CNCTR to choose the targets or themes of its reviews, in line with the challenges and risks associated with surveillance.

The commission carries out around 120 inspections each year. Whilst it does not disclose the number of inspections in each department, this figure is logically determined in proportion to each department's share of the overall intelligence work.

PREPARATION FOR INSPECTIONS AND EXPECTATIONS

Do you control all the intelligence-gathering techniques used by the intelligence services?

It is primarily during the *initial* screening –as part of the processing of applications received by the departments– that legal and technical officers and members of the commission's board flag cases that should be reviewed at a later stage. There is no systematic *retrospective* review of all cases.

Christine, legal and technical officer at the CNCTR

Whilst *ex post* scrutiny covers, proportionally, only a small proportion of the technical surveillance operations authorised under *ex ante* scrutiny, the reports make it possible to identify intelligence-gathering techniques, targets or operations that raise particular concerns and give on-site inspections significant scope.

François, legal and technical officer at the CNCTR

How, then, do you choose which cases to review and the type of review you wish to carry out?

The aim is to verify that data has been used correctly in cases that have come to the Commission's attention, for example:

- where protected professions within the meaning of Articles L. 821-7 and L. 854-3 of the Internal Security Code (CSI): members of parliament, judges, lawyers, journalists;

- where certain techniques are considered to be the most intrusive: collection and recording of computer data, image capture, sound recording. Particular attention is paid both to the grounds for using the technique – verifying that the grounds correspond to the facts already obtained by the service, in particular by examining the raw data and intelligence reports already drawn up, and assessing the relevance of continuing the surveillance – and to its implementation: compliance with the conditions laid down by law, and verification of the link between the purpose and the information gathered by the service.

- Where surveillance operations are of long duration. The oversight body must regularly verify their relevance, that is to say, the continued existence of the threat.

Anne, legal and technical officer at the CNCTR

Inspections are scheduled over a period of several months. This enables us to notify the relevant departments of the dates of our inspections in advance. Each intelligence service is subject to *retrospective* scrutiny, though this is, of course, weighted according to its size and the extent to which it utilises various surveillance techniques. Thus, as you can imagine, the DGSI and the DGSE are subject to more scrutiny than other services such as the National Prison Intelligence Service (SNRP) or the DNRT.

Christine, legal and technical officer at the CNCTR

The oversight exercised by the CNCTR is of a legal nature, but it requires a sound understanding of the threats that justify the various surveillance measures. Consequently, *ex post* oversight provides an opportunity to request a thematic briefing on a specific threat, a geopolitical issue or a matter of internal security. This thematic dimension also guides the selection of topics for discussion and enables the CNCTR to remain relevant in its dialogue with the agencies.

François, legal and technical officer at the CNCTR

A significant proportion of the checks we carry out relate to international surveillance conducted by the first-tier services. These checks are specific because, in this area, only the processing of data is subject to the CNCTR's approval, not its collection. Our role is therefore essentially to verify, on the one hand, that the searches carried out by agency staff within the raw data collected are indeed based on authorisation, and, on the other hand, that the data they extract is essential to the pursuit of the purposes on which the authorisation was based. We are particularly vigilant in ensuring that the surveillance carried out within this framework complies with the limits set by law as regards the national territory. We also verify that the data collected is duly deleted within the time limits imposed by the legal framework, depending on its nature.

The volume and technical complexity of the data analysed in this area require supervisors to use specialised processing tools to identify, amongst the vast number of transactions carried out each day by service staff, any practices that may deviate from the legal framework.

Guillaume, legal and technical officer at the CNCTR

How do you prepare for ex-post controls at the CNCTR? What are your expectations?

Preparation is required before each control. We have to carry out a number of checks:

- first of all, I check the oldest reports so that we can deal with them in a timely manner, after updating the situation and verifying whether the inspection is still appropriate;
- I then check the reports flagged as urgent, so that I can deal with them as a priority;
- For each target where monitoring appears relevant, I carry out a comprehensive analysis of the target in question. I examine their profile, the intelligence-gathering techniques currently authorised –whether or not they are being implemented– as well as the latest information gathered by the service (accessible raw data, intelligence reports), in order to be able to pinpoint the issues at hand and identify the points that the control must highlight, so that I can engage constructively with the service during the control;
- Once the agenda has been drawn up, it is discussed with the deputy project manager who will take part in the control, as well as with the member of the board who will chair it. Where necessary, this discussion leads to changes being made to our agenda;
- The files are then forwarded to the department.

Christine, legal and technical officer at the CNCTR

… But this is not the case for data controls, whether they relate to domestic or international surveillance.

In this type of inspection, it is indeed logical that the commission should be able to examine the records and data exactly as they stand at the time of the inspection. This is a prerequisite for the commission's intervention to be effective.

Nicolas, legal and technical officer at the CNCTR

An control ties up significant resources from the commission, which has few to begin with. It also represents a significant investment for the department concerned. Thorough preparation is therefore essential for a rigorous and effective control. The choice of cases or topics, as well as their number, is important: neither too many nor too few, and the right ones! Whilst a random control is conceivable, particularly in so-called 'data' controls, the logical approach is to start with a reason for the control and then verify its validity and merits.

A member of the commission's panel

Every control is an opportunity to ensure that the direction taken by the services in the implementation of intelligence-gathering techniques remains the right one. The primary objective is assessment, before any observation or criticism. I expect an control to be conducted in this spirit, for the benefit of both the service and the commission.

That said, I must admit that this issue also touches on the auditor's own internal conflict. On the one hand, I dream of an control where everything is in order, of sharing every interpretation of the legal framework with the intelligence officers, and of being nothing more than a spectator to a flawless demonstration of the service's compliance with the rules. But we must admit that an control without a single anomaly leaves a niggling sense of unease: did we target the right areas or search thoroughly enough? And when we uncover a flaw, we experience the paradox of only feeling useful when things are not perfect.

Guillaume, legal and technical officer at the CNCTR

Ex-post monitoring serves a fundamentally legal purpose. However, it also provides valuable information for the Commission, which needs to deepen its understanding of the issues at stake, to understand how the department addresses them and to identify their specific characteristics. This enhances our ability to carry out *ex-ante* monitoring of subsequent applications relating to these issues.

Conversely, the review serves to provide information in the opposite direction, from the Commission to the department. It provides the Commission with an opportunity to give detailed explanations regarding its legal assessment of a particular situation, to clarify what the department may or may not request within the legal framework, and to revisit any unfavourable opinions it has issued, in order to explain its legal analysis.

Generally speaking, the Commission expects, above all, that the *ex-post* review should serve as a forum for dialogue with the department, where everyone can, within their respective roles and with mutual respect, express themselves freely, frankly and confidently, and learn from one another.

Nicolas, legal and technical officer at the CNCTR

How do you prepare for controls within your department, and what are your expectations?

At the DNRT?

For file reviews, as soon as the DNRT receives the agenda, we notify the departments responsible for the intelligence-gathering techniques used in the files under review. We ask them to outline the context in which their target was identified, the benefit to the service, to present the data obtained through the use of authorised intelligence-gathering techniques, to highlight the link to the current threat situation, and to set out the prospects for follow-up: whether or not to continue using intelligence-gathering techniques, depending on the information that remains to be gathered.

We are also liaising with the GIC DNRT to produce a summary for each target based on the transcripts produced (security interceptions and, where applicable, the collection and recording of computer data).

Finally, we are asking the thematic sub-directorates to provide any presentations required by the agenda (new threats, overview of a movement, etc.).

These reviews enable us to freely question CNCTR members on matters of doctrine or on some of their unfavourable opinions or requests for further information, so that we can, where necessary, adapt the reasoning behind our subsequent requests for techniques.

These discussions also provide an opportunity to address the more specific implementation conditions for certain techniques.

For on-site inspections, we prepare them in two stages:

- To begin with, we review the current situation with the section and group heads regarding intelligence-gathering activities, as well as previously submitted requests, refusals received, and planned renewals… In this way, we ensure that we have all the information needed to facilitate a constructive and meaningful discussion with the commission.
  We may also, on occasion, use a specific ongoing case involving technical surveillance to illustrate our work to the delegation and demonstrate the added value provided by the intelligence gathered through such techniques.

- As the meeting approaches, we also check that the various instructions and guidelines are being followed (e.g. conditions and retention periods for transcripts of security intercepts, etc.).

Finally, we decide who will take part in the interview and encourage those selected to prepare a list of questions.

Having prepared in this way, we can approach the control with confidence and derive the greatest possible insights from it.

This can also be an opportunity for staff to seek advice on how to present their requests more effectively. Whilst they may not necessarily meet all expectations, meetings with the CNCTR foster mutual understanding and trust.

Lila, Head of the Legal Division at the DNRT

At the DGSI ?

The DGSI's framework and operating procedures are often the subject of speculation, and the confidentiality inherent in its missions does not always allow it to provide details, in public debate, of its resources and how it operates.

In this context, external and independent oversight is essential to assure citizens that the legal framework is being adhered to. It also presents an opportunity for the DGSI to demonstrate that it is fully implementing this framework.

By granting the commission this power of *retrospective* oversight, the legislator has also created the conditions for dialogue between the intelligence services and the supervisory authority. The DGSI is therefore required to liaise very regularly with the commission's members and special advisers.

The commission organises two types of inspections at the DGSI's headquarters: some focus on the presentation of case files, whilst others – which are more 'technical' – relate to data collected through intelligence-gathering techniques. These are carried out every week at the DGSI's headquarters.

In the first case, the commission provides the list of cases to be reviewed in advance. This procedure enables the DGSI to mobilise, in good time, the investigators responsible for monitoring these cases

– who may be based at head office or in regional offices – and to ensure they are as well prepared as possible for their presentation.

As regards, however, the checks on the data collected, the commission has not provided us with a list of the intelligence-gathering techniques to which it wishes to have access. The DGSI therefore takes no action prior to these checks, and the commission will have access to all the data collected, as it is actually held on the date of its visit.

Marc, head of the DGSI's legal department

The list of cases on which the committee wishes to obtain further details is usually provided one week before the date of the inspection, sometimes less. Whilst the Directorate-General has made arrangements to present the requested information to the committee, this tight deadline does not always allow for the availability of the departments responsible for the cases to be confirmed.

And at the DGSE?

When preparing for controls, we seek to explain to the CNCTR the necessity of intelligence-gathering techniques.

The purpose of these checks is to assure the CNCTR of the transparency and rigour of our authorisation management processes. They demonstrate our commission to handling the sensitive data entrusted to us with the utmost care, as well as our appreciation of the trust placed in our services.

Iris, Head of the Legal Division at the DGSE

Within the department, the proper implementation of Book VIII of the Internal Security Code relies on various channels: a legal unit reporting to the Director of Legal Affairs, which is responsible for monitoring compliance and acts as the Commission's primary point of contact, and a network of legal advisers based across all the department's units.

When an control is announced, it is primarily the responsibility of the legal entity to clarify and specify the CNCTR's expectations. The legal advisers of the organisation that initiated the control are then called upon to prepare for the control. In this context, meetings may be organised to review the subject area covered by the intelligence-gathering techniques under scrutiny or to examine the procedures for using the intelligence-gathering techniques under scrutiny and the data transcribed or extracted. The aim is to clarify the significance of the subject area to which the intelligence-gathering techniques under review relates for the service, as well as the intelligence implications and the value of the technique in question, so that this can be reported to the commission.

Similarly, when a presentation on a specific topic is requested as part of an control, staff are called upon to produce a coherent and comprehensive presentation with a view to the discussion with the commission.

Thus, whilst the network of legal advisers is a key driving force in the preparation of controls, the unit responsible for relations with the commission remains deeply involved in ensuring the consistency of presentations and enabling all the CNCTR's queries to be addressed.

Are you familiar with and do you understand the CNCTR's expectations regarding the inspections it carries out?

For the DGSI

In accordance with the remit assigned to it by the legislature, the Commission issues an opinion on requests to deploy intelligence-gathering techniques, assessing the necessity and proportionality of the technique in light of the infringement it constitutes on the right to privacy. This *ex ante* review is supplemented by an *ex post* review, carried out partly on the Commission's premises and partly at the Directorate-General's offices, in order to ensure that the authorised techniques have been implemented in accordance with the law. In this

context, the Commission verifies that the techniques have been implemented within the time limits and in accordance with the procedures set out in the authorisation, that the retention periods for raw data prescribed by law are being observed, and that the transcripts and extracts produced are relevant to the purposes set out in the law.

This on-site and documentary review is therefore intended to enable the commission to obtain further details or contextual information on a particular case or issue, or to familiarise itself with the information gathered through intelligence-gathering techniques. This *retrospective* review also enables the commission to carry out its *ex ante* scrutiny in full knowledge of the facts: it allows the commission to ascertain how the technique was implemented and what information it yielded, thereby enabling it to assess any application for renewal as effectively as possible.

For the DGSE

The CNCTR must have a clear analysis of the intelligence-gathering techniques under consideration in order to assess their compliance.

In order to improve staff members' understanding of the CNCTR's expectations, the department's legal unit endeavours to clarify its requirements during the preparation of controls. Furthermore, in addition to the publicly available documentation, the department's staff must undertake training on the legal framework in order to be authorised to request intelligence-gathering techniques and to access the analytical tools. This enables staff to gain a better understanding of the commission's expectations during inspections.

For the DNRT

We consider the expectations of the CNCTR, the supervisory authority, to be entirely legitimate. The CNCTR carries out its inspections within

the framework of the remit set out in Articles L.833-1 to L.833-11 of the Internal Security Code.

On-site inspections enable the commission's members to 'get a feel for the situation on the ground' and to gain a better understanding of the challenges faced by the services and their needs in terms of intelligence-gathering techniques. During the interview, we are able to explain to them why we prioritise certain intelligence-gathering techniques over others, depending on the subject matter or the profile of the target in question.

When reviewing case files, we are aware that the commission selects those cases that require closer monitoring on its part, particularly where techniques involving the use of particularly intrusive and resource-intensive methods are employed. Cases involving individuals under long-term surveillance are also subject to special monitoring.

We endeavour to do everything in our power to facilitate the oversight role entrusted to the members of this commission by the legislature, so that this oversight benefits all parties and enables us to enhance the relevance and effectiveness of our intelligence operations.

THE INSPECTION

How are the commission's controls conducted?

Ex-post monitoring is, first and foremost, a forum in which dialogue with the departments takes a more natural form than that resulting from exchanges of classified emails or telephone contacts regarding the day-to-day enquiries handled by our on-call service.

Whilst respecting our respective roles and responsibilities, it is possible to engage in a lively discussion on national security issues and to bring the legal framework to life in the form of a shared responsibility between the regulator and the regulated entity. Beyond the institutional framework established by the legislator, *ex post* oversight is a way of humanising sensitive and sometimes highly technical issues.

The regularity and frequency of inspections also help to facilitate these exchanges by creating a certain 'routine' and a shared memory. In this regard, it is undoubtedly regrettable that the CNCTR's small staff numbers, compared with those of the organisations with which it works, undermine the sustainability of this shared memory. Occasionally, the departure of a legal and technical officer who has gained a good understanding of a department means that links have to be re-established and practices re-adopted which previously facilitated communication on sensitive issues.

François, legal and technical officer at the CNCTR

Controls take place over half a day at the department. When we arrive, the first thing we do is print out the agenda and the preparatory documents for the control from the department being controled. This, in particular, means we do not have to carry sensitive data with us.

We try to manage our time as efficiently as possible, as the controls are intensive and our travel is limited given the small number of legal and technical officer we have.

Christine, legal and technical officer at the CNCTR

In the case of so-called 'data' checks, including those relating to international surveillance, we examine the data held in the services' information systems. We have access to the same data as the services' officers, using the same tools.

In the case of algorithms, the aim is to verify that the actual implementation does indeed comply with the precise description of the processing operation submitted to the Commission for prior approval, in particular with regard to the parameters used in such processing operations. The checks are carried out partly from the Commission's premises and partly directly on the IT infrastructure of the Interministerial Control Group (GIC), on which the processing operations are carried out.

When a potential anomaly is detected, a dialogue is initiated with representatives of the department to confirm whether it has actually occurred and to understand the context, as part of a collaborative process. If the anomaly is confirmed, the department rectifies it and puts measures in place – such as staff awareness-raising or technical safeguards – to prevent the same type of anomaly from recurring.

Guillaume, legal and technical officer at the CNCTR

What is your view of the inspections carried out by the CNCTR?

For the DGSI

More than ten years after its enactment, the Intelligence Act of 24 July 2015 has fully delivered on its promises by safeguarding the work of the intelligence services and providing enhanced democratic safeguards, in particular through oversight by the CNCTR. Its involvement at every stage of the technical intelligence-gathering process is therefore a key component of the framework, ensuring strict compliance with legal requirements.

However, as part of its *ex post* review and discussions with the service's officers, the commission sometimes asks them questions on matters that do not fall within the scope of the review of intelligence-gathering techniques. The DGSI fully understands that the other resources deployed or its investigative strategy may be of interest to the commission and may help it to understand the overall context of a case. However, as these matters do not fall within the scope of intelligence-gathering techniques, the service is unable to provide a response.

For the DGSE

The checks carried out by the CNCTR are not limited to *retrospective* assessment, but also serve as a means of providing support and facilitating progress *from the outset*. This collaborative approach helps to strengthen the legitimacy of the actions undertaken in accordance with fundamental rights and freedoms.

The department views the CNCTR's inspections as a necessary opportunity for face-to-face dialogue with the commission. This framework enables the department to explain its work and improve its internal processes where discrepancies are identified, all within a calm atmosphere characterised by mutual understanding.

However, within the department, staff could organise annual themed presentations to promote a better understanding of the DGSE's highly specialised remit.

For its part, the Commission could present a medium-term work programme covering several themes, which would provide a clearer understanding of its areas of focus and the rationale behind its work. Indeed, some requests for presentations or explanations are sometimes made at short notice, and the department occasionally finds it difficult to link certain requests to the CNCTR's core remit.

The service would like to see an increase in requests for presentations on specific topics, which would enable it, on the one hand, to set out the context of its work and its requests for intelligence-gathering techniques and, on the other hand, to discuss with the commission the best way to ensure that its requests are proportionate to the issues at stake.

It has noted an increase in the number of requests for technical presentations and for information on how analysis tools operate, sometimes on subjects which it considers to be of limited significance.

However, it should be emphasised that responsibility for compliance with Book VIII of the Internal Security Code must not rest solely with the tools – even though the service makes significant efforts to ensure that these tools are designed to facilitate such compliance – but lies with the agents themselves. This is why the DGSE pays particular attention to the training of its officers, to internal oversight and to addressing deviant behaviour through the implementation of a code of conduct.

Finally, given the sensitive nature of the matters dealt with by the service, the relevance of questions that sometimes relate to the operational implementation of certain techniques or to matters falling outside the Commission's remit –particularly in the context of controls– may be called into question. The DGSE's expertise is, in fact, also deployed beyond our borders and must therefore be rigorously protected from our enemies through strict compartmentalisation of information and strict adherence to the need-to-know principle.

For the DNRT

On-site inspections, whether at head office or in the regions, give us the opportunity to 'put faces to the names' of the CNCTR's members, and humanise a commission that can sometimes seem distant, Parisian, and perhaps out of touch with the realities on the ground.

The CNCTR members therefore strike us as approachable and attentive to the difficulties we face. The inspections do not cause the DNRT any particular concern.

Consistent in their interpretation of the Internal Security Code and steadfast in their case law, discussions with the Commission's members are generally constructive and sometimes offer a glimpse of different 'approaches' to considering a case. Once these have been explained and set out, we gain a better understanding of the Commission's stance and remit.

What do the CNCTR's inspections bring to you?

At the DNRT

For us, as officers working in the regions, these checks are genuinely important and much appreciated, as they enable us to be involved in the discussions.

Field officers, who have in-depth knowledge of the cases and utilise intelligence-gathering techniques, never have direct access to the CNCTR. They have their requests approved by their line managers before the request is forwarded via the DNRT's one-stop shop. The DNRT then carries out checks on both the substance and form of the requests before they are passed on to the approval chain. There are therefore numerous intermediaries. These checks thus provide us with an opportunity to clarify any regulatory points that we consider to be unclear.

Asking our questions without going through the DNRT as an intermediary sometimes makes it easier to reach a mutual understanding of both specific cases and broader issues. This enables us to discuss the difficulties we face directly with the commission, or to raise their awareness of specific requests that are currently being processed or are due in the future. These direct exchanges also allow us to highlight the specific characteristics of a region in terms of safeguarding the nation's fundamental interests and to convey certain messages, or even grievances.

Every region has its own specific characteristics. National threats arise within specific contexts and are linked to local issues. Whilst they may seem trivial at national level, they are nonetheless very real and tangible at local level.

Antoine, a superintendent at a regional branch

During territorial checks, the departmental territorial intelligence services, given the volume of intelligence-gathering techniques they employ, would sometimes like to be granted more time.

Headquarters briefings, meanwhile, provide an opportunity to present the service's priorities to the commission or to highlight new threats or emerging trends. Usually delivered by an analyst specialising in the subject, these presentations benefit both the commission and the DNRT's single point of contact for all its intelligence-gathering techniques.

These reviews enable us to freely question CNCTR members on matters of doctrine, or on certain decisions to reject applications or requests for further information, so that we can, where necessary, adapt the arguments put forward in our subsequent applications for authorisation of techniques. These discussions also provide an opportunity to raise more specific issues regarding the conditions under which certain techniques are implemented.

Prior to an inspection, we believe it would be useful to be able to bring specific situations to the CNCTR's attention, such as cases where raising the service's awareness would be helpful, or others where a request for intelligence-gathering techniques has been unsuccessful. The commission could thus draw on concrete examples familiar to the service to help us improve both the substance and the form of our requests.

Time could also be set aside for the service's priority areas, particularly where these are new and where intelligence-based investigations are difficult to carry out.

Whilst they may not necessarily meet all expectations, meetings with the CNCTR foster mutual understanding and trust.

For the DGSE

The purpose of these checks is to ensure that the CNCTR can be confident in the transparency and rigour of our authorisation management processes. They demonstrate our commitment to handling the sensitive data entrusted to us with the utmost care, as well as our appreciation of the trust placed in our services.

These controls provide the department with an opportunity to outline the scope of its remit and priorities. They help to clarify the department's working methods and dispel any potential ambiguity regarding their implementation, thereby ensuring that the commission can be confident in the transparency and rigour of our work.

These reviews also provide a better understanding of the CNCTR's expectations and facilitate a genuine dialogue on any differences in interpretation. In turn, the department expects the CNCTR to understand the issues at stake in the case and for the department, and to provide it with advice. The department then implements the recommendations and advice issued by the commission, in order to strengthen the legitimacy of its actions.

This is an opportunity to reiterate that our work is carried out within a strict procedural and legal framework, ensuring compliance with the law.

These inspections primarily provide an opportunity to explain the agency's missions and requirements within a complex and ever changing geopolitical context, thereby highlighting the need to carry out operations aimed at gathering intelligence of interest.

This educational exercise helps to clarify the context of the requests made by the DGSE. It can also serve as a forum for clarifying interpretations of certain provisions and highlighting residual needs not covered by the existing regulatory framework.

The CNCTR's interventions provide an external perspective on operational matters that may sometimes be dealt with as 'routine' business.

As well as providing a better understanding of the requirements relating to the application of Book VIII of the Internal Security Code, these controls –which can sometimes represent a significant workload– help to raise staff awareness of the procedures to be followed and to identify areas where improvements can be made.

We regularly present topics to the commission, which enables the service to educate the commission, thereby familiarising it with the service's intelligence challenges and demystifying the DGSE's operations. This exercise serves to demonstrate the professionalism and rigour of the service's officers.

This framework can also help to anticipate differences in interpretation before intelligence requests are made and to justify operational requirements.

Internally, this enables officers to make an effort to explain their research work in layman's terms and to take a step back from their usual practices when viewed from the commission's external perspective.

For the DGSI

Our department has always regarded the CNCTR's oversight as going beyond a mere check on compliance with the legal framework to constitute a genuine opportunity for dialogue. The relationship of trust established with the Commission since 2015 has enabled a constructive dialogue to be initiated between the DGSI and its supervisory authority, with a view to reconciling the legal framework with technical and operational requirements.

This relationship is essential for exchanging views and thus striking the right balance between monitoring compliance with the legal framework and the DGSI's ability to carry out the tasks entrusted to it effectively in order to protect the nation's fundamental interests.

In addition to the grounds for the requests and any requests for further information, the discussions held during on-site inspections enable the DGSI to provide the commission with additional details necessary to assess the necessity and proportionality of an intelligence-gathering techniques and to raise its awareness of certain issues.

Direct discussions with the commission enable us to obtain clarification on certain opinions it has issued or on the commission's doctrinal positions.

This gives us the opportunity to raise the Commission's awareness of the operational context of our requests. We can thus discuss the Commission's positions and opinions on the use of intelligence-gathering techniques and propose, whilst always complying with the legal framework, changes that would enable us to meet the technical or operational requirements faced by investigators.

The Commission's opinions and recommendations arising from this dialogue thus provide officers with a clear and reassuring framework for the use of intelligence-gathering techniques.

Furthermore, in addition to carrying out inspections on its premises, either at the request of the commission or on its own initiative, the DGSI is regularly called upon to give thematic presentations to the CNCTR's board. These may, for example, involve outlining the nature of a new threat that the service has identified.

Presentations made at the request of the CNCTR are most often in connection with specific cases or current events. By providing an assessment of the threat and contextual information, they shed new light on the cases compared with the grounds set out

in the applications for authorisation of the techniques. These briefings therefore offer the DGSI an additional channel through which to explain its needs, particularly with a view to renewing authorisations or implementing new techniques.

As part of an ongoing dialogue, the DGSI endeavours to respond favourably to the Commission's requests for briefings on a systematic basis.

AFTER THE INSPECTION

From the agencies' perspective, what do you do after the inspections?

At the DNRT

In the regions, inspections are followed by an internal debriefing, covering how the inspection was conducted and areas for improvement, so that all staff can benefit from the information and advice provided. We then work to ensure the swift implementation of, and follow-up on, any recommendations or issues identified by the CNCTR.

At central level, a memo is drawn up for the attention of senior management, whilst a message is sent to each department whose case was raised during the control, in order to inform them of the CNCTR's comments; for example, to explain the need to provide further information if the department wishes to renew applications for the use of intelligence-gathering techniques that have been in place for some time.

If aspects of the CNCTR's doctrine are discussed during the inspection, they will also be shared with the departments that are required to request intelligence-gathering techniques within the directorate, as well as with decentralised departments and field officers, *via* email, guidance sheets (on a specific type of technique or purpose), or even through memos. The CNCTR's doctrine is also reiterated in the DNRT's internal general instruction on the implementation of techniques.

At the DGSE

An control report is drawn up and circulated to all relevant staff, setting out the guidelines to be followed.

Within the department's units, an control report is drawn up and then circulated to the staff concerned, in order to clarify the commission's expectations, set out its recommendations and set out the actions to be taken. The aim is to ensure the swift and thorough implementation of requests for improvements and to provide staff with better training to prevent a recurrence of the inconsistencies identified.

Analysing any irregularities reported by the CNCTR enables staff to identify deviations from best practice and current regulatory requirements.

Within the department, staff take the feedback provided by the CNCTR *via* their legal adviser very seriously. The irregularities identified enable staff, for example, to spot discrepancies between current practices and the applicable regulatory requirements, thereby helping them to better incorporate the legal framework into their work.

Dealing with any anomalies in international surveillance is complex, as the anomalies identified by the CNCTR may come to light several weeks or even months after the agent's operation. This does not necessarily allow the agent to provide a precise and context-specific response to enquiries. In domestic surveillance, the handling of the rare anomalies is, from the service's point of view, satisfactory.

At the DGSI ?

The DGSI endeavours to put into practice the discussions held with the CNCTR during its inspections.

Following a control, a report is drawn up and the commission's observations are systematically communicated to all the departments concerned. The staff responsible for monitoring and implementing the intelligence-gathering techniques that have been controled are thus informed of the commission's feedback. In most cases, this serves to reinforce their confidence in their practices. In other cases, the commission's queries may lead them to make certain adjustments, such as providing further details on specific points in the justification for requests for such techniques. Any areas for improvement suggested by the commission are monitored to ensure they are properly taken into account.

Nevertheless, the predominantly written procedure for dealing with anomalies disrupts the flow of dialogue. Supplementing this with oral discussions would therefore enable the DGSI to provide answers to certain queries more quickly and to discuss any points of disagreement more freely.

As for the CNCTR, what do you do following the controls?

A report is drawn up after each control by the legal and technical officer who carried out the control. It is finalised by the member of the panel who led the control. It is then reviewed by our colleague responsible for coordinating *ex-post* controls and, from 2026, by the department's lead officer. Finally, the report is reviewed by the chairman and the secretary-general of the commission. Where appropriate, it will be circulated to the other members and to the other legal and technical officer.

These minutes reflect our discussions with the department, and we aim to set out in them the answers we received to the questions we had raised prior to the control.

It also serves as a record of any irregularities identified during the control, which will subsequently be notified to the department, which will be asked to respond. We adhere to the principle of the right to be heard, which is inherent in any control process. In this way, the service may also be asked to take measures that the Commission has deemed necessary in light of its findings. This may, for example, involve the destruction of data that has been retained even though, as it is unrelated to the stated purpose for implementing the intelligence-gathering techniques, it is not essential to the investigation being conducted by the service.

Data checks also enable the commission, with the assistance of the service, to refine its understanding of the mapping of the data held by a service. This knowledge forms the basis of our understanding of how data is stored and processed by each intelligence service.

Anne, legal and technical officer at the CNCTR

Ex-post review is a key stage in a case officer's work cycle: it enables them to consolidate their understanding of the threats and challenges justifying the use of intelligence-gathering techniques, to inform the assessment of the requests processed daily by our on-call service, and also to ensure

that the Commission fulfils the mandate entrusted to it by law: to help ensure that the services comply with the legal framework.

In this regard, the handling of anomalies identified during reviews is a major challenge.

It is indeed not enough simply to identify discrepancies without ensuring that corrective measures are put in place. However, addressing anomalies requires several elements: firstly, a common understanding of the legal framework applicable to the case in question, which usually occurs without the need for conflicting interpretations; secondly, a smooth and effective channel of communication to ensure that anomalies are addressed: a corrective measure applied months later is of little use; and finally, consistency in findings and analyses, enabling both parties to strengthen their controls by ensuring the predictability of the consequences arising from each type of anomaly identified. It is clear that all of this is particularly time-consuming!

François, legal and technical officer at the CNCTR

Ex-post monitoring, which forms an integral part of the CNCTR's remit, is systematically addressed in the Commission's annual public report, covering both quantitative and qualitative aspects, through a review of the irregularities identified and the recommendations made by the Commission.

Nicolas, legal and technical officer at the CNCTR

RELATIONS BETWEEN THE CNCTR AND GOVERNMENT DEPARTMENTS

How do you view relations with the members and project officers of the CNCTR?

For the DNRT :

This is a relationship based on trust; the CNCTR has a supervisory role, but also an advisory one, and a balance must be struck between the need to use the requested technique and the necessary respect for the purposes and the principle of proportionality.

In this relationship, we do not wait for an control to report an anomaly. We notify the CNCTR as soon as we become aware of it. This was, for example, recently the case when we reported the loss of a tracking device.

As regards the DGSE :

Relations with the CNCTR are constructive and smooth.

Within the department, relations with the CNCTR are primarily managed by the legal entity reporting to the Director-General. Department staff only meet with the commission's members and legal and technical officer on an occasional basis, during presentations at the time of inspections.

In this context, officers report that working relationships are conducted in a serious and non-confrontational atmosphere. These discussions are intended to prevent policy officers from interpreting the law too strictly when issuing guidelines, to the detriment of the service's operational requirements.

How do you view relations with the intelligence services?

For the past ten years, the primary aspect of our relationship with the intelligence services has been trust, and it must remain so.

Our position differs from that of the services but is not opposed to it, since both the CNCTR and the services are required to apply the law.

The knowledge and professionalism of the people we deal with are very often remarkable. There is a genuine concern for compliance with the law at every level. We must bear this in mind.

We appreciate the support provided by the relevant departments during the controls we carry out. We also devote considerable resources to this. Therefore, whilst discrepancies or disagreements are a natural outcome of the control, in this area as in others, we must make the most of our respective investments by subsequently taking the necessary steps to find solutions and make progress.

A member of the CNCTR's board

Relations with the security services must be courteous and frank. The security services work to protect the fundamental interests of the nation, and the Commission ensures that the legal framework adopted by the citizens' representatives is properly applied. The Commission's oversight of the security services' activities is intended to strike a balance between the protection of the nation as a whole and that of the individuals who make it up.

Christine, legal and technical officer at the CNCTR

The fundamental assumption underpinning my dealings with the services is that they, like the Commission, are strictly law-abiding. The Commission monitors procedures, not the services as a whole; consequently, inspectors do not have unlimited access, and an inspection is not a search. If a service were to deliberately lead the inspectors on a tour of a Potemkin village, it would no doubt succeed in doing so for a time, at its own risk. Consequently, the aim is not to catch the service red-handed, but to provide assurance that the rules are being followed and to identify any irregularities so that the service can rectify them: the objective is a shared one.

Conversely, I expect the services to trust in our ability to handle their information confidentially, with discretion, and with a view to improvement rather than punishment.

It is natural that the total commitment of intelligence service officers to their mission should shift their perception of the right balance between protecting the nation's interests and individual freedoms: dialogue with the commission enables us, beyond simply clarifying regulatory expectations, to maintain that balance.

Nor am I unaware of the risk that the services might reveal only the bare minimum, which would enable them to obtain the CNCTR's endorsement for practices that are, in reality, on the fringes of the legal framework. This is why the inspections retain a certain investigative element, with a view to making an informed assessment of what is presented to us.

Guillaume, legal and technical officer at the CNCTR

What is particularly striking is the diversity of the relationships between the commission and each department: they vary according to the size, organisational culture and key contacts within each department. Some make it a point of honour to respond as quickly and comprehensively as possible to any issues, whilst others take less care. Some departments regularly contact the commission directly by telephone or secure email in advance of potential difficulties to seek advice, whilst others simply submit their request and wait to see if it elicits a response.

Nicolas, legal and technical officer at the CNCTR

Appendices

Changes in the composition of the college during 2025

The composition of the CNCTR's board changed during 2025.

Indeed, as mentioned in the 2024 report, following the resignation of President Lasvignes in January 2025, Ms. Solange Moracchini was appointed acting president[66], and then, by decree of 28 March 2025,

Mr. Vincent Mazauric was appointed chairman of the commission[67]. Furthermore, on 31 August 2025, the term of office of Mr. Philippe Distler, a qualified member of the CNCTR, came to an end. He was replaced by Mr. Jean-Marc Détré.

At the end of 2025, the CNCTR's board comprised the following **nine members**:



- **Mr. Vincent Mazauric**,
  Member of the Council of State, Chairman;



- **Ms. Émilie Bonnivard**,
  Member of Parliament for Savoie;

66. See the decree of 31 January 2025 issued by the President of the Republic, appointing Ms. Moracchini, a member of the Board, as acting Chair with effect from 1 February 2025.

67. See the decree of 28 March 2025 of the President of the Republic appointing the Chair of the National Oversight Commission for Intelligence-Gathering Techniques, published in the Official Journal on 29 March 2025



- **Mr. Christophe Naegelen**,
  Member of Parliament for the Vosges;



- **Ms. Chantal Deseyne**,
  Senator for Eure-et-Loir;



- **Mr. Jérôme Darras**,
  Senator for Pas-de-Calais;



- **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**,
  concellor at the Court of Cassation;



- **Mr. Jean-Marc Détré**,
  General of the Gendarmerie (2S),
  Qualified expert in electronic communications.

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 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.

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

- **Collection and recording of computer data (RDI)**

  Physical or remote access to data collection and recording of 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.

- **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 purpose.

  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 purpose 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 collection and recording of computer data 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 and recording 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.

Partial translation generated by AI and checked by CNCTR.



Hôtel de Cassini - 32 rue de Babylone - 75007 Paris
https://www.cnctr.fr/

Layout : DSAF / SDIMP / BAEC / Section Édition (np) - 22 October 2026 - ISSN 2268-5278