COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

8e 2023 Activity Report

Foreword

Intelligence to fight crime...

21,000 people were under surveillance in 2022 in France. 24,000 were in 2023. Fundamentally, this was probably an expected change. It is the result of the growing threats to our country. Its analysis by surveillance purpose however holds some surprises in store.

The numerous international crises of course significantly increase the number of people under surveillance to counter interference. In the same way, the increasing terrorist threat on French soil combined with the scattering of possible perpetrators, often young isolated individuals explains why the number of "targets" has increased so much.

However the most notable change is not linked to any of those two purposes. It is due to the rise in the number of people monitored as part of the prevention of organised crime. For the very first time, the prevention of terrorism is not the first purpose in terms of number of targets. The extent of the administrative police's involvement in a field that used to be in the remit of the judicial police demonstrates that the threat linked to drug trafficking has nowadays become a challenge for the good working of the institutions.

An ineluctable escalation of monitoring techniques

The number of requests to use intelligence-gathering techniques sent to the Commission has continued to grow: 95,000 requests in 2023. This increase (+6% compared to the previous year) is however lower than that in the number of people under surveillance. Indeed, the administrative monitoring with a view to preventing organised crime does not last as long and requires fewer techniques when a terrorist group is being monitored: as soon as suspicions have been confirmed, the judicial authority takes over.

The Commission makes sure of this

The ever increasing use of the most intrusive techniques is more significant than this increase in volume terms. Placing microphones in private property, collecting all the computer data of an individual, tapping phones and computers: there are attempts to offset the currently low contribution of traditional wire-tapping. This escalation looks inescapable, since the people being monitored (in particular violent extremists) are more and more aware that they might be under technical surveillance and able to protect themselves from that. Some strict framework is therefore necessary.

But, unlike wire-tapping, centralised with one department of the Prime Minister (GIC, the inter-ministerial control group), the particularly intrusive techniques are directly linked to requesting divisions. The product of wire-tapping is stored and handled thanks to systems belonging to those divisions. The Commission has access to this with difficulty, since the law does not grant it direct access to those systems, unlike the provisions pertaining to data kept by the inter-ministerial control group. Moreover, its control is complex, given the volume and heterogeneous nature of collected data.

There is therefore a risk that the control would gradually weaken.

Towards improved control

The Commission strongly highlighted this risk in its previous report. This did not go unheeded. On the instructions of the President of the French Republic sent to the National Intelligence and Counter-Terrorism Coordinator, the technical division of the Directorate-General for External Security (DGSE) worked in close conjunction with the technical division the General Directorate for Internal Security (DGSI) The aim is to help the inter-ministerial control group centralise all the data gathered thanks to the computer data collection technique, thus help it play its role of "trustworthy third-party" in full, by 2027. The Commission will have remote access to it, for control needs, as well as the divisions to handle its contents.

The Commission welcomes this huge step forward. It can be added to the progress made with the help of the divisions in the field of the facilitation of controls, in particular for international surveillance. This progress complements the discussions with the divisions, but does not replace it: the human dimension of controls, the Commission considers the discussions it makes possible to be irreplaceable.

Make the rule of law a reality...

The rule of law is not something that should be taken for granted. It is a tension, a quest, that demands that the law be continuously adjusted to the reality on the ground. And intelligence oversight is no different. Thus, the 2025 law-making meeting[1] may be the opportunity to round out a legislative framework, which has fundamentally proven its worth. In the interest of good administration, the Commission thought it useful to help prepare this meeting and underline in this report an array of aspects that might justify an intervention of the law-maker. I would like to underline here those that would help better safeguard rights.

The way the right to recourse for people afraid they are being under surveillance without any lawful reason can be improved. The law however states that the Commission, called upon by any individual, checks that no intelligence-gathering technique has been unlawfully implemented with regard to them. The number of those complaints almost doubled in 2023. But the Commission's "checking" capacities come across the ban imposed on it to access the so-called "sovereignty" files, including should the latter be likely to accumulate the results of the intelligence-gathering techniques, as per a questionable interpretation of the law. The checking is therefore not exhaustive.

1. See Section 3.2 of this report here below.

The unhappy complainant is able to bring the matter before the Council of State (*Conseil d'Etat*). However, the explanations the Prime Minister services and the Commission provided to the judge are covered by National defence secrecy, the claimant cannot have access to the file. However, it does not appear impossible to find some compromise between protection of secrecy and compliance with the adversarial nature of the jurisdictional procedure, for example by drawing inspiration from the British procedure and allowing the claimant to call upon a lawyer who would be chosen from among a very small number of specially authorized lawyers.

We will also recall the question of the control of data exchanges between French services and their foreign counterparts, a control which we know is necessary to meet the requirements of the European Court of Human Rights, but which we differ, year after year, the legislative translation, pending a decision from the Court regarding the French legal framework, a decision of which we do not know when it will be introduced, and if it will deal with this subject.

Finally, in the very near future, the issue of artificial intelligence appears. A tool that intelligence cannot do without. It is also a challenge for the law-maker, who is already wondering whether a decision will be made about the surveillance of an individual according to criteria of which no human will know either the content or the weighting with certainty... So it seemed legitimate that the Commission makes its particular contribution to the current flow of reflections. This is the subject of a study that can be found in the "Insights" section of this report. Similarly, this section provides a contribution from the French Ambassador for Digital Affairs, who alludes to France's international efforts towards the necessary regulation of cyber-intrusion devices.

...and give legal certainty to services.

It is normal and necessary for the legal framework to be the subject of adjustments, either during a legislative modification, or as a result of an evolution of the Commission's doctrine on the conditions of application of the law. But intelligence services, like businesses, also need to benefit from what lawyers call legal certainty: the positions of the Commission shall be found easily, clearly stated and well disseminated; changes to the doctrine shall be sufficiently predictable; their impact shall be assessed through prior discussion with the services involved.

The Commission is fully committed to implementing these principles. It has enhanced the dialogue with the services, both to better characterize the threats, accurately assess the legitimacy of the requests, and to be informed of the effects of certain positions that it proposes to adopt. It has also consolidated its doctrine and prepared a suitable dissemination system. It has chosen, within the various departments, people open to constructive dialogue.

There is reason to hope that the reduction in 2023 in the share of negative opinions issued on requests for techniques (1.2% compared to 1.6% the previous year) is at least partly the result of this approach.

Serge LASVIGNES
Chairman of the CNCTR

2023 Key figures

94,902
requests for intelligence-gathering techniques
(domestic)

24,209
people under surveillance

150
collegial meetings

136
controls
in the divisions

€3.1 million
in budget

15 travels
to the territories
including **in an overseas department**

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

20 agents
(on 31/12/2023)

- 9 men / 11 women,
- 12 public agents / 8 contract agents,
- average age of 39 years.

2023 Activity Report

Section 1. Overview of surveillance in 2023: an increase in the number of people under surveillance and the techniques implemented in connection with the rise of certain threats

As in its previous reports, the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR) reports on the carrying out of its mission to ensure that intelligence-gathering techniques are implemented in compliance with the legal framework governing them, by publishing information as detailed as national defence secrecy allows on its control activity and by providing the public with its findings on how services use intelligence-gathering techniques against people present on the French soil.

In the provided overview of a five-year period, these elements relate to the number of people under surveillance, the purposes[1] mentioned in support of the requests for intelligence-gathering techniques submitted to the Commission as well as the number of opinions issued about these requests for authorisation.

The Commission also reports on the number of prior opinions it issued in 2023 on requests relating to international electronic communications monitoring.

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

The statistical elements provided in this report come from some work on data extraction and aggregation carried out by the CNCTR jointly with the Inter-Ministerial Control Group (GIC), then on improved data reliability.

1.1. Sharp increase in the number of persons under surveillance, which should not conceal divergent trends depending on the purpose for which the monitoring is carried out.

As it has done since its first activity report, the Commission has calculated the number of people who were the subject in 2023 of at least one intelligence-gathering technique, among those provided for in Chapters I to III of Title V of Book VIII of the French Internal Security Code. Authorisations to access pre-recorded internet connection data which are limited to allowing the identification of subscribers and the index of subscription numbers are not taken into account[2].

After an almost 9% decrease in 2022, the number of people under surveillance this year amounts to 24,209, i.e., up more than 15% compared to 2022, and of 9% compared to the period before the health crisis linked to the Covid-19 pandemic.

2. The CNCTR indeed considers that the identification of subscribers and the index of subscription numbers, provided for in the second paragraph of Article L. 851-1 of the French Internal Security Code, constitute less of a surveillance measure strictly speaking than a prerequisite for surveillance measures. In the opinion of the Commission, such measures begin from the moment the "phone records" of the involved individual are received as per the first paragraph of the same Article L. 851-1.

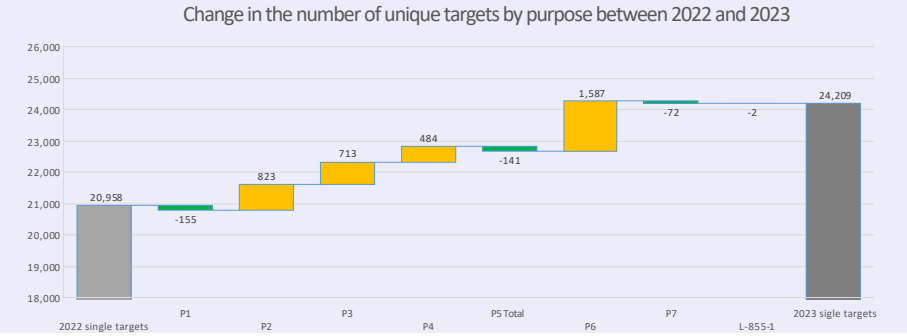
	2019	2020	2021	2022	2023	2022/2023 change	2019/2023 change
Number of people under surveillance	**22,210**	**21,952**	**22,958**	**20,958**	**24,209**	**+ 15.5 %**	**+ 9 %**
For terrorism prevention purposes	**7,736** (34.8 % du total)	**8,786** (40 % du total)	**7,826** (34.1 % du total)	**6,478** (30.9 % du total)	**6,962** (28.8 % du total)	**+ 7.5 %**	**- 10 %**
For purposes linked the prevention of organised crime	**5,693** (25.6 % du total)	**5,021** (22.9 % du total)	**5,932** (25.8 % du total)	**5,471** (26.1 % du total)	**7,058** (29.2 % du total)	**+ 29 %**	**+ 24 %**
For the purpose provided for in Article L. 811-3 (5) of the French Internal Security Code[3]	**3,021** (13.6 % du total)	**3,238** (14.8 % du total)	**3,466** (15.1 % du total)	**2,692** (12.8 % du total)	**2,551** (10.5 % du total)	**- 5.2 %**	**- 15.6 %**

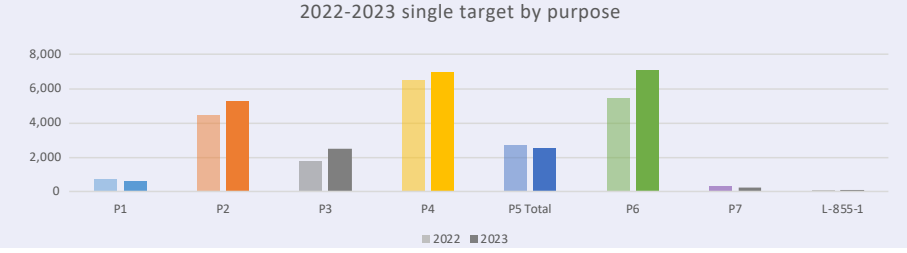
This increase in the number of people under surveillance is linked to changes in the nature and intensity of the threat. It mainly results from unprecedented investment in the prevention of organised crime as well as a fight against the various forms of interference (1.1.1.). On the other hand, the prevention of various forms of violent activism (purposes mentioned in point 5° of Article L. 811-3 of the French Internal Security Code), a field in which the issue of protecting privacy is combined with an issue of protecting freedoms of speech, opinion, association or even demonstration, experienced a slight decrease for the second year in a row (1.1.2).

3. I.e., the prevention of: a) attacks on the republican form of institutions; b) actions aimed at maintaining or rebuilding groups dissolved in compliance with Article L. 212-1; c) collective violence likely to seriously harm public peace.

1.1.1. A sharp increase in the number of people monitored in correlation with the evolution of the current threat: the prevention of organised crime becomes the first purpose for surveillance in terms of the number of people involved

The graphs below make it possible to observe both the way in which the increase in the number of people monitored is broken down into the various purposes[4] and the evolution of this figure for each of these purposes between 2022 and 2023.





(P1): purpose 1, national independence, territorial integrity and national defence;

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

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

(P5): the prevention of: a) attacks on the republican form of institutions; b) actions aimed at maintaining or rebuilding dissolved groups; c) collective violence likely to seriously harm public;

(P6): the prevention of organised crime;

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

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

4. It should be emphasized that a given person can be monitored for several purposes, the total difference observed between 2022 and 2023 does not correspond to the aggregation of the differences observed for each purpose.

Data for 2023 firstly highlight an increase of a little more of 29% in the number of people under surveillance for the **prevention of organised crime** (purpose 6). This significant increase can be explained both by a growing control of techniques by specialized services and by their increased effort, particularly with regard to the fight against drug trafficking, which has become a major issue in terms of public security in the matter of a few years. The increase noted in 2023 is consistent with a 24% increase in the number of people monitored for this purpose since 2019 (+42% since 2016)[5]. Beyond that, the extent of the issue also results from the fact that this year, more people were monitored for this purpose than for the prevention of terrorism.

With regard to the purpose relating to the **prevention of terrorism** (purpose 4), the number of people monitored increased by 7.5% in 2023 in correlation with the rise of both exogenous and endogenous risks in a very volatile international context; the occurrence of terrorist attacks on French soil compelled intelligence services to reassess the current threat.

Despite the overall downward trend over a longer period (-10% of people monitored compared to 2019, - 22% compared to 2016[6]), the increase observed in 2023 highlights the resurgence of the threat in the matter as well as its shape-shifting nature, this being increasingly linked to isolated individuals, who can hastily act and whose monitoring or resumed monitoring affects the activity of the services.

The volatility of the international context, in particular due to the war in Ukraine since 2022 and the resuming of the Israeli-Palestinian conflict in the second half of 2023, can also explain the increase in the number of people under surveillance for the **purpose relating to the major interests of foreign policy, the execution of France's European and international commitments and the prevention of any form of foreign interference** (purpose 2).

5. 4,969 people were monitored for the prevention of organized crime and delinquency in 2016, accounting for 24.4% of the total people monitored at that time. See the second 2017 CNCTR activity report, p. 54.

6. 9,475 people were monitored for terrorism prevention purposes in 2016, accounting for 46.5% of all people under surveillance that year. See the second 2017 CNCTR activity report, p. 54.

Finally, the number of people under surveillance for the **defence and promotion of France's major economic, industrial and scientific interests** (purpose 3) is also increasing but reaches the same level as that observed in 2019[7] before the start of the health crisis.

Regarding these last two purposes, this slightly upward trend is consistent with that already observed last year.

1.1.2. Well-attested decrease in the number of persons monitored as part of the prevention of violent extremisms and collective violence

Like the trend noted in 2021 and 2022, the fall in the number of people monitored for the purpose provided for in 5° of Article L. 811-3 of the French Internal Security Code is confirmed with a drop by 5.2% compared to 2022. The number of people under surveillance for that purpose reached its lowest level since 2018[8].

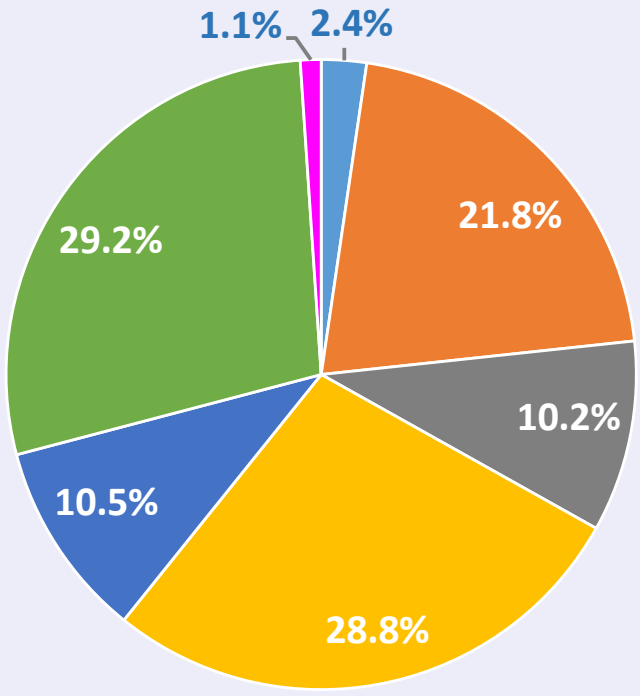
This change, which is accompanied by a downward trend in the number of negative opinions issued by the Commission on requests for techniques, is undoubtedly connected to the approach chosen by the Commission in 2023, in order to better explain the outline of this purpose and better disseminate its doctrine, particularly through the thematic study focusing on this specific subject as part of its previous activity report, a classified version of which was sent to the services. This initiative made it possible to create a particularly constructive dialogue with them which led to more accurate targeting of people of interest[9].

7. See the 4th 2019 CNCTR activity report, p. 57 and following.

8. 2,116 people were monitored as part of the purpose referred to in Article L. 811-3 (5) of the French Internal Security Code in 2018. See the sixth 2021 CNCTR activity report, p. 73.

9. On this point, see the study relating to the monitoring of violent extremists appearing in the seventh 2022 CNCTR activity report, p. 75 and following.

Breakdown of monitored people depending on the purposes behind the monitoring



Note: One given person may be monitored for several purposes, the various aggregated percentages exceed 100%.

METHOD FOR CALCULATING THE NUMBER OF PEOPLE UNDER SURVEILLANCE

The number of people under surveillance is calculated by the CNCTR thanks to data shared by the Inter-Ministerial Control Group. This data comes from various computerised processing operations which help process requests for intelligence-gathering techniques based on the data for which the Prime Minister was granted an authorisation during the year when the study was drawn up.

The results of this calculation, however, include a margin of error given various constraints.

Indeed, the processing of requests for intelligence-gathering techniques uses various applications; this leads to the aggregation of data which is, even today, not completely harmonised, even if the year 2023 made it possible to improve this harmonisation in the field of real-time geolocation[10]. Furthermore, requests from the services are made by intelligence-gathering technique mentioned in the French Internal Security Code and not by individual. In addition, the people targeted are not always named or precisely identified.

To mitigate the risk of "duplicate" resulting from these various technical and operational constraints, the Commission has developed an algorithmic approach based on the comparison of the elements present in requests of techniques, such as information linked to the personal information about the targeted person. but also the IDs linked to the devices targeted by the intelligence-gathering technique (for example the number of the tapped telephone). These comparisons help identify people who have a number of IDs in the various bases made available by the Inter-Ministerial Control Group for the calculation and to remove "duplicates".

Finally, the calculated indicator, i.e., the number of targets monitored, has a margin of error that the CNCTR estimates at less than 10%. However, the Commission is currently working on possible changes to its calculation method in order to make the results obtained more reliable.

10. Intelligence-gathering technique provided for in Article L. 851-4 of the French Internal Security Code.

1.2. A continuous increase In the number of requests for monitoring techniques made

In 2023, the total number of requests for the implementation of intelligence-gathering techniques on the national territory is 6% higher than that in 2022. This increase is much lower than that in the number of people under surveillance (+ 15 %). The growth difference can undoubtedly be widely explained by the fact that the increase in the number of people monitored is mainly due to the prevention of organised delinquency. In fact, surveillance in this field is shorter: either it is unsuccessful and is stopped (or not renewed), or it quickly leads to a referral to the judicial authority. Moreover, the services which are mainly responsible for this make less use of multiple techniques (excluding identification services, the average number of techniques requested per person monitored for this purpose is approximately 1.6 while it is 3 for the purpose of preventing terrorism).

It should be kept in mind that the CNCTR issues an opinion on each request aimed at implementing an intelligence-gathering technique on French soil before the Prime Minister makes his decision[11]. It must rule within twenty-four hours when a request falls within the jurisdiction of a member having the status of magistrate[12] and ruling alone. This deadline is extended to seventy-two hours when this request needs to be examined as a collegial, plenary or restricted committee[13]. The CNCTR endeavours to observe those deadlines.

Furthermore, as explained in the Commission's previous activity report, a so-called "priority" procedure was introduced to meet operational needs calling for the urgent processing of requests. It allows opinions to be usually issued within less than one hour[14].

11. See the seventh 2022 CNCTR activity report, p. 132.

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

13. In accordance of the provisions of Article L. 832-3 of the French Internal Security Code, the collegial committees of the Commission shall in particular deal with any new or serious question. The plenary collegiate committee meets at least once a month and is particularly competent to hear requests relating to protected professions.

14. See the 7th 2022 activity report, pp. 16-17 about this topic.

1.2.1. Opinions issued on domestic surveillance: well-attested increased use of the most intrusive techniques

In terms of domestic surveillance, the opinions issued by the CNCTR are broken down as follows

These figures take into account all requests submitted by the intelligence services between 2019 and 2023.

They help highlight changes over five years and from one year to the next in the way services use each category of techniques.

	2019	2020	2021	2022	2023	2023 / 2023 change	2019 / 2023 change
Access to recorded internet connection data (identification of subscribers and the index of subscription numbers) (Article L. 851-1 of the French Internal Security Code)	25,051	30,758	32,254	31,427	33,657	+ 7.1 %	+ 34.4 %
Access to recorded internet connection data (other requests, including linked to "phone records") (Article L. 851-1 of the French Internal Security Code)	14,568	18,006	19,974	19,263	21,430	+ 11.2 %	+ 47.1 %
Real-time access to internet connection data (Article L. 851-2 of the French Internal Security Code)	1,184	1,644	1,534	1,175	763	- 35.1 %	- 35.6 %
Real-time geolocations (Article L. 851-4 of the French Internal Security Code)	7,601	8,394	9,920	10,901	10,982	+ 0.7 %	+ 44.5 %
Security intercepts through the Inter-Ministerial Control Group (Article L. 852-1 of the French Internal Security Code)	12,574	12,891	12,736	12,798	13,021	+ 1.7 %	+ 3.6 %
Tapped communications using *IMSI catcher*[15] (II of Article L. 852-1 of the French Internal Security Code)	0	0	0	0	0	-	-

15. This relates to technical systems used to collect internet connection data of terminals, particularly the numbers of SIM cards or IMSI (*International mobile subscriber identity*)

	2019	2020	2021	2022	2023	2023 / 2023 change	2019 / 2023 change
Security intercepts on exclusively wireless networks (Article L. 852-2 of the French Internal Security Code)	3	0	3	5	10	+ 100 %	+ 233.3 %
Collecting of correspondence sent or received through satellite (Article L. 852-3 of the French Internal Security Code)	0	0	0	0	0	-	-
Location of people or objects ("geotagging") (Article L. 851-5 of the French Internal Security Code)	1,793	1,598	2,006	1,951	2,084	+ 6.8 %	+ 16.2 %
Collecting of internet connection data using *IMSI catcher* (Article L. 851-6 of the French Internal Security Code)	288	311	583	641	607	- 5.3 %	+ 110.8 %
Recording of words spoken in a private capacity and recording of images in a private setting (Article L. 853-1 of the French Internal Security Code)	3,282	1,564	2,138	3,314	3,802	+ 14.7 %	+ 15.8 %
Collecting and recording of computer data (Article L. 853-2 of the French Internal Security Code)	3,591	2,418	3,758	4,260	4,493	+ 5.5 %	+ 25.1 %
Entering of private places (Article L. 853-3 of the French Internal Security Code)	3,599	2,021	2,682	3,767	4,053	+ 7.6 %	+ 12.6 %
All the requests for intelligence-gathering techniques	73,534	79,605	87,588	89,502	94,902	+ 6 %	+ 29.1 %

This data shows that after having somewhat increased in 2022 (+2.2%), the total number of requests for the implementation of intelligence-gathering techniques increased by 6% in 2023, closer to the annual changes for 2020 and 2021.

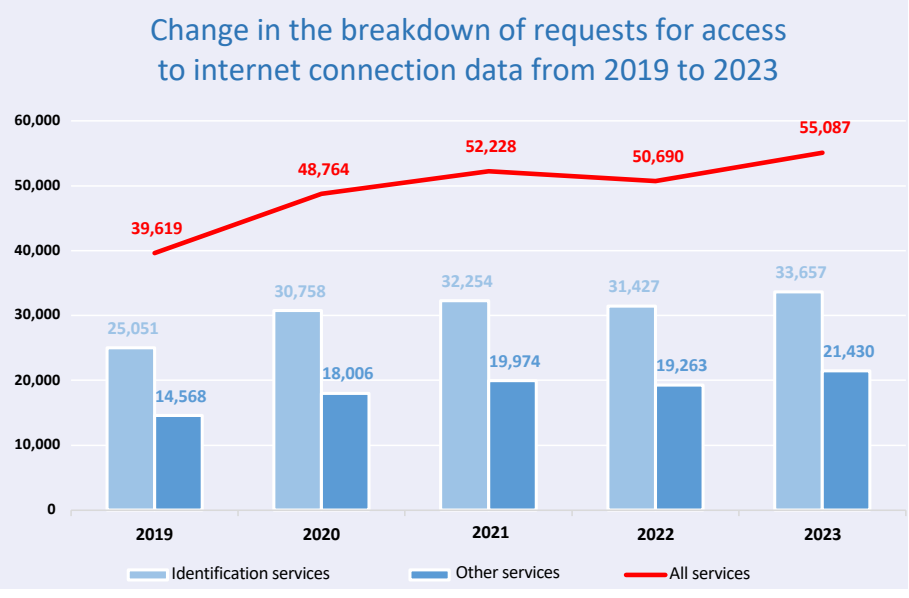
With the exception of real-time access to internet connection data and the collection of internet connection data using IMSI-catcher, this increase takes into account all the intelligence-gathering techniques covered by the French Internal Security Code, in more or less different proportions.

Access to technical internet connection data is still the first-line monitoring technique by far.

As in previous years, **the requests for access to recorded internet connection data**, which are less intrusive compared to other techniques, remain the reference techniques. They rose by 9% in 2023 after the 2022 decrease.

This upward trend is the result of the increase in the number of people under surveillance, these techniques being somehow first-line techniques. It is also explained by the diversification of the services requested from the Inter-Ministerial Control Group, now including in particular data linked to the use of social media.

It should be kept in mind that when applying the Commission's calculation method, a request is likely to relate to several accesses at the same time. Thus, a request to identify a person's telephone subscription numbers may result in collecting several numbers from several electronic communications providers and, therefore, the issuance of several requests.



However, **the requests for real-time access to internet connection data**, which dropped in 2019 and 2020, continue to significantly decrease: -35% this year, after a 23% drop in 2022. This smaller use of this technique perhaps results from the fact that it is, as per the provisions of Article L. 851-2 of the French Internal Security Code, limited to the purpose of preventing terrorism.

Monitoring techniques whose intrusive nature can be described as intermediate are increasing moderately.

The number of **real-time geolocation requests** stabilised in 2023 (+ 0.7%), after five years of growth, resulting in a 45% increase between 2019 and 2023. This technique, which enables the surveillance of the target's movements without physically mobilising agents, is also a reference technique now well-known and mastered by the services.

Requests for **security intercepts** ("tapping") made via the Inter-Ministerial Control Group have also been rather stable over the last five years. 13,021 requests were submitted in 2023, compared to 12,798 in 2022 (+1.7%).

This small increase can undoubtedly be associated with the technical quota provided for by Article L. 852-1 of the French Internal Security Code, which did not change in 2023. It is also probably linked to some self-regulation of services with regard to the resources which must be committed to handle these intercepts.

The use of techniques for locating people or objects ("tags") has remained stable over the last three years, i.e., with approximately 2,000 requests per year.

The use of the most intrusive monitoring techniques continues to significantly increase.

Techniques for the **recording of words spoken in a private capacity and the recording of images in a private setting** continue to significantly

increase. If we ignore the sharp decline in 2020 and 2021 linked to the Covid-19 pandemic, we see that between 2019 and 2023, requests for these techniques increased by almost 16%. This development is obviously directly related to the lower productivity of telephone tapping linked to the use of encrypted or secure messaging.

According to the same logic, the **technique for the collecting and recording of internet computer data** (RDI) also experienced a significant increase in 2023 (+5.5%), although lower than that observed in 2022 (+13.4%). Over the 2019-2022 period, this is an increase of more than 25% in the use of this technique.

Furthermore, a new authorization to implement automated processing meant to detect connections likely to reveal a terrorist threat (so-called **algorithmic** technique, provided for in Article L. 851-3 of the French Internal Security Code) was granted in 2023, i.e., bringing the number of algorithms authorized since the implementation of this technique to intelligence services in 2015 to 5. The option created by Law No. 2021-998 of 30 July 2021 pertaining to the prevention of acts of terrorism and intelligence to extend the algorithmic technique to the full addresses of resources used on the internet (Uniform Resource Locator, URL)[16], however, has not yet been implemented.

On the other hand, the **collecting of internet connection data using IMSI catcher** was lower in 2023 with 607 requests, compared to 641 in 2022, i.e., a 5.3% drop. This decline must nevertheless be put into perspective in view of the significant increase in the use of the technique (+110%) over the whole of the 2019-2023 period.

The reduction in the use of IMSI catchers in 2023 is mainly due to the operational constraints involved in the effective implementation of the devices or technical systems involved.

16. See Article 15 of the law, which amended Article 851-3-1 of the French Internal Security Code.

1.2.2. Increase in the number of operation authorisation requests regarding international electronic communications monitoring

In 2023, the Commission issued 3,981 opinions on requests for the exploitation of intercepted international communications, compared to 3,715 in 2022, i.e., a 7% increase. The change in the number of opinions issued by the CNCTR regarding monitoring requests of international electronic communications over the 2019-2022 period is detailed in the table below.

	2019	2020	2021	2022	2023	2023 / 2023 change	2019 / 2023 change
Number of opinions issues in the field of international electronic communications monitoring	**2,133**	**4,316**	**4,374**	**3,715**	**3,981**	**+ 7.2 %**	**+ 86.6 %**

THE LEGAL FRAMEWORK OF INTERNATIONAL MONITORING

The international electronic communications monitoring is governed by the provisions of Articles L. 854-1 to L. 854-9 of the French Internal Security Code. The articles state that specialised intelligence services may be authorized to handle communications sent or received from abroad, intercepted on electronic communications networks listed by the Prime Minister.

These “handling” authorisations are issued by the Prime Minister, after consultation with the CNCTR. Several categories of authorisations are provided for, depending on the purpose and scope of the surveillance considered. This may involve monitoring communications sent or received within a geographic area, by an organization, by a group of people or by a single person.

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

Subject to exceptions expressly provided for by law, individual surveillance of communications of people using "national" numbers or IDs (i.e., "French" communications) is prohibited. Should such communications be intercepted, they shall be destroyed immediately.

1.2.3. Number of negative opinions however decreasing as a result of improved dialogue between the divisions

In a way that may seem counter-intuitive at first glance, the increase in the number of people monitored and the number of requests for intelligence-gathering techniques did not lead to an increase in negative opinions issued by the Commission. On the contrary, the number of negative opinions experienced a significant 20% drop (775 negative opinions compared to 974 in 2022), all techniques combined, compared to 2022. Excluding requests for internet connection data, the rate of negative opinions accounts for 1.2% of total requests compared to 1.6% in 2022.

This result can undoubtedly be explained by the improved knowledge of the legal framework, with significant training work carried out by the services and the Commission's policy for consolidating and disseminating its doctrine. It is also linked to more exchanges between the Commission and the services either before the transmission of a request considered sensitive, or during its investigation, at the initiative of the Commission.

In its 2019 and 2022 activity reports[17], the CNCTR explained how it enriched the procedure for examining requests provided for by law by reserving the possibility of inviting services to complement the

17. See the 7th 2022 CNCTR activity report, p. 28 and following.

motivation for their requests in order to assess more easily both the necessity and the proportionality of the means requested in relation to the interests of the person involved.

These requests for additional information may relate both to the substance of the files and to the concrete implementation of the techniques envisaged, so as to remove any ambiguity and to fully measure the impact of the measures envisaged on the people targeted or their immediate environment.

This very important tool in the context of ex-ante controls makes it easier to distinguish between requests the motivation of which cannot comply with the framework for the use of techniques provided for by law and requests the wording of which is inaccurate or ambiguous.

However, while the number of these requests for additional information had very significantly increased in 2022, this increase continued at a high level in 2023 with an increase of more than 21% regarding techniques other than internet collection data.

	2022	2023	2022 / 2023 change
Intelligence-gathering techniques (excluding internet connection data)			
Opinions issued	**38,830**	**39,848**	**2.6 %**
Requests for additional information	**1,134** (i.e., 2.9 % of the total)	**1,373** (i.e., 3.4 % of the total)	**+ 21.1 % (0.5 pt)**
Negative opinions	**629** (i.e., 1.6 % of the total)	**496** (i.e., 1.2 % of the total)	**- 21.1 % (-0.4 pt)**

All intelligence-gathering techniques combined			
Opinions issued	**89,520**	**94,935**	**6.0 %**
Requests for additional information	**2,582** (i.e., 2.9 % of the total)	**2,797** (i.e., 2.9 % of the total)	**+ 8.3 % (0 pt)**
Negative opinions	**974** (i.e., 1.1 % of the total)	**775** (i.e., 0.8 % of the total)	**- 20.4 % (-0.3 pt)**

A WORKING METHOD FOCUSED ON EXCHANGE AND COMMUNICATION

Dialogue with services is essential for mutual understanding and the implementation of an adequate and effective control.

If requests for additional information remain the basic tool of these exchanges, the CNCTR also relies on new means for disseminating information.

Thus, the services are regularly invited to present, to the members of the CNCTR, the themes, strategies and difficulties encountered as part of their action, whether physically within the premises of the Commission, or recently through secure video conferences for more ad-hoc interventions.

In return, the sharing of the CNCTR doctrine with the services is the subject of particular attention, with the introduction of systematic dissemination early 2024, through alert sheets and an annual letter.

Finally, the cornerstone of the relationship between the Commission and the services, the ex-post controls carried out in situ make it possible to address all the subjects via the action of the "referent" project managers of the service involved.

1.3. The purposes invoked in support of requests for the implementation of intelligence-gathering techniques: a distribution very similar to that observed in 2022

Using the presentation adopted in each of its activity reports, the CNCTR lists, for all requests aimed at the implementation of an intelligence-gathering technique relating to domestic surveillance[18], the proportion of each of the seven purposes listed in Article L. 811-3 of the French Internal Security Code[19]. This breakdown of techniques according to purpose does not coincide with that of the people under surveillance.

Indeed, depending on the purpose pursued, the average duration of surveillance of targeted people varies greatly, as does the number of techniques implemented. In concrete terms, the surveillance of a person monitored for the prevention of terrorism requires on average more techniques than that of a person monitored for the prevention of organised crime[20].

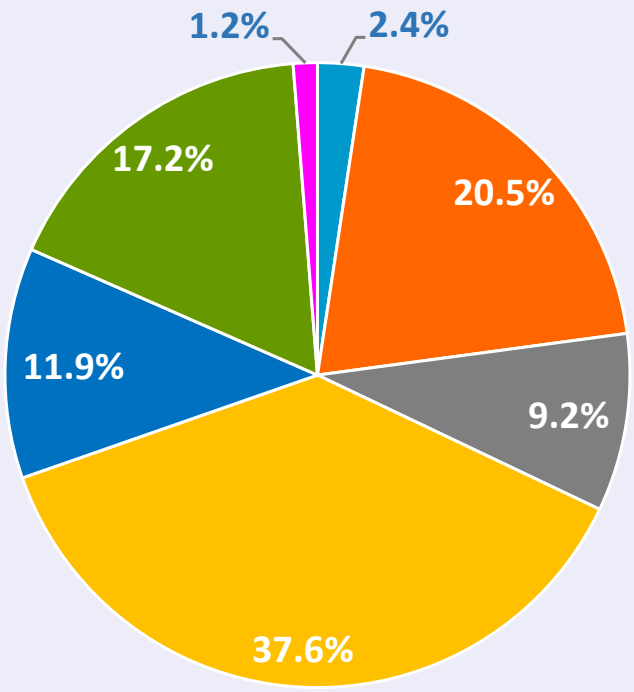
The following graphs present, for the first, the share taken by each of the purposes provided for in Article L. 811-3 of the French Internal Security Code in the total number of requests and, for the second, the change in the total number of techniques requested by purpose over the last four years.

18. These are the techniques provided for in Chapters I to III of Title V of Book VIII of the French Internal Security Code.

19. It should be noted that in addition to the seven purposes mentioned in Article L. 811-3 of the French Internal Security Code, Article L. 855-1 of the same code provides access, for the sole benefit of the national prison intelligence-gathering service (SNRP), to a limited number of techniques for its own purpose, namely the prevention of prison breaks and the maintenance of security inside the prisons and health facilities to receive prisoners. In 2023, this purpose was invoked in 0.1% of requests for the implementation of intelligence-gathering techniques, this proportion being identical to that recorded in 2021 and 2022. Given the very low figure, this purpose, which only involves one service, does not appear in the established diagrams.

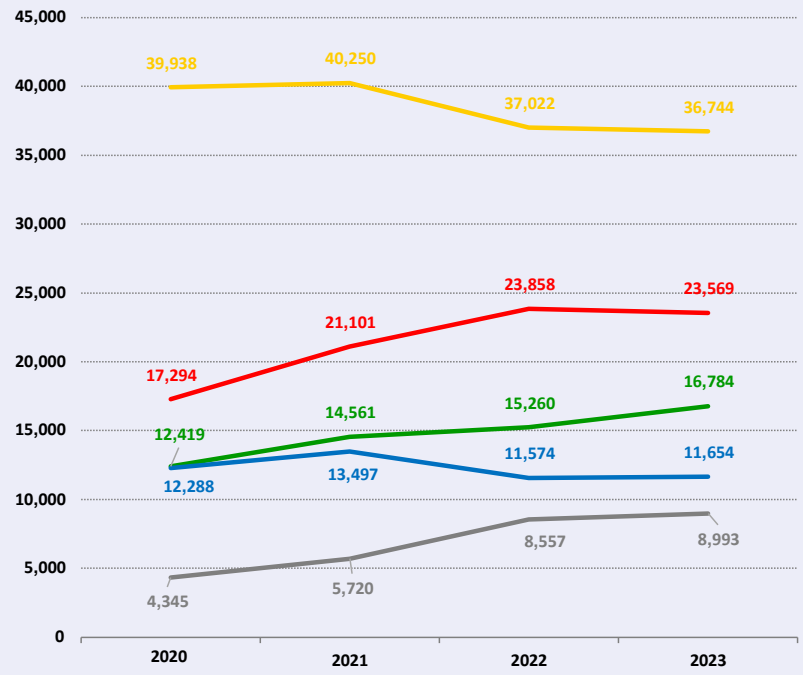
20. See point 1.2 above, p. 30.

Purposes mentioned in support of requests for intelligence-gathering techniques in 2023



- 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 damage to the republican form of institutions, actions aimed at maintaining or rebuilding dissolved groups, and collective violence likely to seriously harm public peace
- Prevention of organised crime
- Prevention of the proliferation of weapons of mass destruction

Change in the number of requests per purpose used between 2022 and 2023



Prevention of terrorism

France's geostrategic interests (national independence and defence, major interests of foreign policy and prevention of any form of foreign interference, fight against the proliferation of weapons of mass destruction)

Prevention of organised crime

The prevention of damage to the republican form of institutions, actions aimed at maintaining or rebuilding dissolved groups, and collective violence likely to seriously harm public peace

The major economic, industrial and scientific interests of France

1.3.1. The prevention of terrorism remains the most frequently provided purpose (in number of requests)

Since 2015, the number of intelligence-gathering techniques requested as part of the prevention of terrorism remains significantly in the lead even if it tends to stabilise after the sharp increases in 2020 and 2021.

The share of this purpose among all the techniques requested has slightly decreased since 2020 and now stands at 37.6%.

1.3.2. A stabilisation of the number of requests submitted for purposes linked to France's geostrategic interests

Requests for intelligence-gathering techniques based on the three purposes relating to **France's geostrategic interests**[21] sharply increased in 2020 and 2021. In 2023 they remained at a level comparable to that observed last year, namely just under 24,000 requests (23,500 requests compared to 23,800 in 2022).

This relative stability at a high level results, as last year, from the international geopolitical context with the emergence, in various geographical zones, of armed conflicts with worldwide impact, and from espionage activities carried out by foreign services on French soil, which remain at a sustained level.

A detailed examination of this group of purposes also reveals that the number of requests based on the purpose mentioned in 2° of Article L. 811-3 of the French Internal Security Code, i.e., the prevention of any form of foreign interference, after having significantly increased in 2022, continues to decrease.

21. This aggregate combines the purposes provided for in points 1°, 2° and 7° of Article L. 811-3 of the French Internal Security Code, namely: 1) national independence, territorial integrity and national defence; 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; and 7) prevention of the proliferation of weapons of mass destruction.

1.3.3. Slight rise in the number of requests for techniques based on the prevention of organised crime linked to the sharp increase in the number of persons monitored in this respect

As in 2022, the prevention of organized crime and delinquency comes in third position in the ratio of purposes invoked by the services in support of their requests, with a share of 17% of authorizations granted. The total volume of techniques requested for this purpose continues to increase. With a 10% increase in requests based on this purpose in one year, their number rose this year to 16,800 compared to 15,200 in 2022, thus reaching their highest value over the last five years, reflecting the intense activity services in this area.

1.3.4. Stabilising of the number of requests based on the prevention of collective violence despite the slight fall in the number of persons monitored in this respect

The number of requests made for the prevention of collective violence remains stable at 11,600. However, this stabilisation of the number of techniques requested should be linked to the drop in the number of people monitored under this purpose (see point 1.1 above) reflecting better targeting of persons of interest by the services with the corollary of more intensive surveillance using an increased number of techniques.

In this regard, the CNCTR recalls that it is particularly vigilant regarding the motivation of requests submitted on the basis of the purpose mentioned in paragraph c of 5° of Article L. 811-3 of the French Internal Security Code, considering that the prevention of collective violence cannot be interpreted as a vector of interference in a political or trade

union environment or of limitation of the constitutional law to express one's opinions, even if they are extreme, as long as the risk of violence likely to seriously harm public peace is not sufficiently plausibly alleged.

As an expression of this increased vigilance, most negative opinions issued by the Commission in 2023, like in previous years, involved this purpose. However, the CNCTR notes that the rate of negative opinions issued tends to decline while the number of requests for this legal purpose remains stable.

As specified in its previous activity report, the Commission carried out significant work to formalise and consolidate its doctrine, materialised in the form of a regularly updated collection and serving as a reference within the framework of ex-ante control of requests. The dissemination of its section devoted to the prevention of collective violence within the intelligence services contributed to the reduction in the number of negative opinions issued in this matter.

Finally, the number of requests submitted on the basis of **defence and the promotion of France's major economic, industrial and scientific interests**, remains relatively stable compared to 2022.

Economic exchanges having now returned to their level before the health crisis, competition between States, exacerbated and sometimes aggressive, as well as the high risk of collecting strategic information in economic, scientific and technological matters lead to a significant involvement of services working on this issue.

Section 2. Ex-post controls of intelligence-gathering technique use significantly reinforced, which underlines the recurrence of anomalies with varying levels of seriousness

The ex-post control carried out by the Commission over the activity of intelligence services has a threefold dimension. The first step is to understand the flow of data collected using intelligence-gathering techniques and their operating conditions. Secondly, its purpose is to check the conformity of the use made of this data with a particular issue when protected professions within the meaning of Articles L. 821-7 and L. 854-3 of the French Internal Security Code are involved. Finally, it also has an informative, educational and relational dimension to help better understand the challenges of the service and the reality on the ground by being in direct contact with operational staff but also to clear up the inevitable misunderstandings that may arise.

This ex-post control is a crucial issue in the face of the fear of a growing gap between, on the one hand, the limited resources of the CNCTR and, on the other, the use of increasingly intrusive devices to record huge quantities of data with no comparison with what it was "at the time of phone tapping", the use of increasingly sophisticated pre-processing and processing systems for this data and the complexity and the diversity of their storage conditions.

This reality resulted in the strengthening of ex-post control, which is a strategic priority at this stage of the life of the Commission, with better selectivity and improved follow-up of the correction of detected anomalies.

2.1. More regular, better targeted and more effective ex-post controls

2.1.1. | Unprecedented level of control within the divisions

With 136 documentary audits and on-the-spot inspections carried out in 2023, regardless of the division, the Commission achieved, with virtually constant human resources[22], the highest level of ex-post controls since it was created in October 2015.

This evolution is based in particular on a very significant increase in the number of controls devoted to surveillance measures in the field of international electronic communications monitoring. Thus, 42 controls were carried out on this topic regarding the six so-called "first-line" intelligence services[23], to be compared with the thirty controls carried out in 2022 and the twenty controls carried out in 2021.

This very strong increase over two years can be explained by a change in the concrete control methods towards less formalism and more technical computer verifications, allowing a smaller body of the Commission to access, within each service, a dedicated computer workstation providing access to data collected on the basis of the provisions of Articles L. 854-1 *et seq.* of the French Internal Security Code. During these checks, verifications focus on the data collected and the handling operations carried out to limit the involvement of agents of the service in charge.

Requests for justification of any anomalies detected are sent at the end of the inspection via a secure communication channel.

22. If three new positions in the Commission were allowed for the 2023 financial year (see the seventh 2022 CNCTR activity report, p. 134) and as a result, two new mission manager positions could be created and a fourth full-time college member in particular to enable a greater number of on-the-spot inspections to be carried out, the new theoretical count of 14 project managers was in practice only reached during two weeks in 2023 due to people leaving and recruitment difficulties already reported in the previous annual report.

23. The specialised intelligence services, the so-called "first-line" services, cover the Directorate-General for External Security (DGSE), the General Directorate for Internal Security (DGSI), the National Directorate of the Intelligence and Customs Investigations (DNRED), the Directorate of Military Intelligence (DRM), the Directorate for Defence Security and Intelligence (DRSD) and the nationally competent service known as "processing of intelligence and action against clandestine financial circuits" (TRACFIN).

Regarding the 94 controls devoted to so-called domestic monitoring techniques, about 80 were carried out in the premises of central administrations, mainly those of the so-called first-line services, and, as in 2022, around fifteen were carried out inside the facilities of the services or the Inter-Ministerial Control Group, including overseas[24].

2.1.2. New possibilities for remote control and follow-up for better targeted and more efficient control

Furthermore, these figures do not reflect the development of the Commission's remote capabilities during the year as well as its follow-up and in-depth capabilities.

Indeed, as a continuation of the evaluation of its ex-post control methods carried out in 2022[25], the Commission acquired new secure communication and remote control tools.

In its premises, the Commission now has a secure video conferencing tool, workstations with remote access to intercepted so-called mixed international electronic communications[26] and, to a still very modest extent, means of access to certain data collected by sound or video devices, or from authorised collecting of computer data.

2.1.3. Improved presence in the territories

Over the past year, the CNCTR has carried out around fifteen visits to the facilities run by the Inter-Ministerial Control Group as well as to the service locations in the provinces (see the inserts below).

24. See point 1.2.3 below.

25. See the 7th 2022 CNCTR activity report, p. 56 and following.

26. These are communications referring to subscription numbers or technical IDs that can be associated with the national territory.

Maintaining a high volume of these trips in the territories, since it is 50% higher than that experienced by the Commission before the health crisis of 2020-2021, helps make its desire to better understand local issues and difficulties intelligence services a reality; but it also helps ensure control of the entire chain of requests and implementation of intelligence-gathering techniques.

The purposes of travels have also evolved in a similar way. While they mainly aimed at allowing the Commission to meet local managers of decentralized intelligence services, in order to discuss the reality of intelligence issues in their respective regions and the difficulties encountered in the application of the legal framework, they are now associated with data control actions and compliance with legal and regulatory procedures.

These travels now take place in two ways: either as part of an Inter-Ministerial Control Group centre, or directly in the service premises.

CONTROLS CARRIED OUT IN THE INTER-MINISTERIAL CONTROL GROUP'S FACILITIES

These controls consist of a series of interviews, carried out with each decentralised service, generally beginning with a presentation of the current state of the threats affecting the territory concerned and their possible specificities, then moving to an assessment of the intelligence-gathering techniques implemented by the services involved and the results obtained.

These discussions make it possible to talk about certain opinions issued by the Commission and to explain the related elements of doctrine. The services can also take the opportunity of these meetings to bring technical or legal difficulties to the attention of the Commission and discuss their work prospects.

Finally, the Commission sometimes takes advantage of these trips to meet major local security players, prefects or public prosecutors, when subjects or specificities justify it.

CONTROLS IN LOCAL SERVICE FACILITIES

Implemented in the second half of 2022, these controls within the sites of the services on French soil, appeared necessary for the Commission, in addition to travelling to the territorial sites of the Inter-Ministerial Control Group, both to perfect its knowledge of the organization and the functioning of services and intensify its control.

In practice, these local controls can be implemented in a specific service based on a decision of the chairman or the college when an irregularity is suspected, or be carried out in several services upstream or downstream of a trip to the Inter-Ministerial Control Group's centre to which they report.

During these trips, in addition to exchanges that may be similar to those held in Inter-Ministerial Control Group's centres, an in-depth control of the procedures for implementing intelligence-gathering techniques, storage of materials used for the collection of sensitive data (such as microphones, tags, IMSI-catchers or concealable cameras) and data stored locally is carried out.

The proper keeping of the various registers provided for by the French Internal Security Code or the regulations arising from Articles 226-3 and R. 226 *et seq*. of the French Criminal Code[27] is also, where applicable, verified.

These trips are also an opportunity to ensure that agents responsible for implementing intelligence-gathering techniques have a good understanding of the legal framework. They also help verify that the materials used for gathering intelligence are stored in such a way as to limit their access to authorised agents only and that precise traceability overseen by an appropriate line manager guarantees their use in accordance with the law.

Finally, data checks, carried out directly on sensors or certain raw data processing computers, allow to ensure that the services do not have stocks of information which would deviate from the rules imposed on centralisation and deadlines for storage and traceability.

27. Article 226-3 of the French Criminal Code provides for a penalty of five years of imprisonment and a fine of €300,000, in particular for "*The manufacture, importation, possession, exhibition, offer, rental or sale of devices or technical equipment likely to be used to carry out operations which may constitute the offence provided for in the second paragraph of Article 226-15 or which, designed for the remote detection of conversations, make it possible to carry out the offence provided for in Article 226-1 or whose purpose is the collecting of computer data provided for in Articles 706-102-1 of the French criminal procedure code and L. 853-2 of the French Internal Security Code and appearing on a list drawn up under conditions fixed by decree in the Council of State, when these acts are committed, including by negligence, in the absence of a ministerial authorisation, the conditions of grant of which are defined in the said decree or without complying with the conditions defined in this authorisation*". Articles R. 226-1 *et seq.* define the terms and conditions under which these devices are subject to authorisation and set up a consultative commission, in which a representative of the CNCTR participates, the secretariat of which is provided by the National Systems Security Agency. information (see Article R. 226-2).

In total, as in previous years, the CNCTR draws up a usually satisfactory assessment of the documentary audits and on-site inspections that it carried out in 2023. The discussions with the services as part of the preparation of these controls are very fluid and easy, and the conditions in which the Commission's teams are welcome in the premises of the services do not call for any observation.

However, as the Commission had the opportunity to point out in its previous reports and despite the measures taken to develop the conditions of ex-post control, the human and material resources at its disposal remain a limiting factor while the number of intelligence-gathering techniques implemented and the mass of data collected continues to increase.

Furthermore, in the concrete organization of its on-the-spot controls, the CNCTR is sometimes faced with logistical and technical difficulties (availability of access, complexity of networks, difficulties in locating data, etc.) which must lead the services to pursue the actions they have been working on since 2023 to guarantee full access to the data collected by the implementation of intelligence-gathering techniques and to the results of their handling. Finally, the Commission considers that, when it involves methods of collecting information of a particularly technical nature, the effectiveness of its control, both ex-ante and ex-post, presupposes increased knowledge of the possibilities provided by the techniques used, and the methods of processing the data collected. In this regard, it intends to continue to support technical dialogue that was established with the services in 2023 without calling into question the imperative of preserving the confidentiality of the operating methods that they develop.

2.1.4. Development of the control also resulting from the increasing number of complaints from private individuals without this leading to an increased referral to the specialised division of the Council of State (*Conseil d'Etat*)

The CNCTR can be contacted by any person who wishes to verify that no intelligence-gathering technique is or has been irregularly implemented against them[28].

The power of verification that the law has granted to the Commission relates only to the intelligence-gathering techniques provided for by the French Internal Security Code, namely techniques implemented by intelligence services as part of their administrative police missions. This competence does not extend either to surveillance measures ordered by the judicial authority or to those, moreover illegal, carried out by private individuals.

For reasons of national security, and in application of the provisions of Decree No. 2015-1405 of 5 November 2015 relating to exceptions to the application of the right of users to contact the administration electronically, the CNCTR can only be validly contacted by letter sent by post. The complaint shall be presented by the person involved, providing proof of their identity, and specifying the technical IDs based on which they wish the checks to be carried out. These technical elements, in particular telephone numbers or e-mail addresses, shall be supplied along with supporting documents, such as a subscription contract or an invoice. Verifications can only take place when all of these information items and supporting documents have been communicated to the Commission.

28. This prior complaint procedure is provided for by the provisions of Article L.833-4 of the French Internal Security Code with regard to national surveillance and by those of Article L. 854-9 of the said code, with regard to the international electronic communications monitoring.

The CNCTR examines the complaints it receives in the same way and using the same tools as when it carries out an ex-post control on its own initiative from its premises.

Significant increase in the number of complaints

After some relative stability in previous years, the number of complaints received by the CNCTR in 2023 increased by more than 65%.

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

If the reasons behind such an increase cannot be fully identified, the publication of the new CNCTR website, on 15 June 2023, and more particularly of a page dedicated to the terms of referral to the Commission (*https://www.cnctr.fr/saisir-la-commission*) has undoubtedly had an impact on the number of complaints submitted.

This impact can also be observed when studying the comprehensive nature of the requests for verification received In fact, the rate of requests sent to the CNCTR that could be examined without having to submit a request for additional documents increased from 18.37% in 2022 to 34.38% over the 2023 period following the publication of the website.

Regarding multiple complaints, three people submitted more than one complaint in the course of 2023 and six complainants who had already contacted the CNCTR in the past asked that verifications be carried out about them again.

As in previous years, the response time to complaints providing all the necessary information items for their processing was significantly less than two months[29].

29. This period runs from the date on which the complaint is ready to be examined. When a request for additional documents (proof of identity, proof of subscription, etc.) has been sent to the author of the complaint, this period only begins to run from the moment these documents are received.

No complaint led the CNCTR to send any recommendation to the head of the intelligence service involved, to the minister they report to or to the Prime Minister asking for the implementation of a technique to be suspended and collected intelligence destroyed, in compliance with Article L. 8336 of the French Internal Security Code.

THE SYSTEM SPECIFIC TO "WHISTLE BLOWERS"

To ensure that potential clear violations of the legal framework applicable to intelligence-gathering techniques are brought to an end, Article L. 861-3 of the French Internal Security Code provides that agents of the intelligence services having knowledge, in the exercise of their functions, of such a violation, may bring these facts to the attention of the CNCTR only. It is then up to the Commission, in view of the elements it was sent, to use, where appropriate, the control powers assigned to it by law.

These provisions have not been implemented since the coming into force of the legal framework in 2015.

A recourse to the judge which remains rare

The special contentious procedure provided for in Articles L. 773-1 *et seq.* of the French Code of Administrative Justice makes it possible to ask that a specialised body of the Council of State verify that no intelligence-gathering technique is or has been unlawfully used against an individual. The members and the public rapporteur of the specialised body are authorised in their capacity to know information covered by national defence secrecy.

With regard to intelligence-gathering techniques relating to domestic surveillance, the specialized body of the Council of State may be contacted, on the basis of Article L. 841-1 of the French Internal Security Code, by any individual who can justify having previously exercised their right to complain before the CNCTR.

With regard to measures to monitor international electronic communications, only the chairman or at least three members of the Commission can refer the matter to the Council of State. The domestic surveillance regime, however, applies if the verification concerns the legality of the exploitation of communications of individuals using IDs linked to the national territory and communicating from France. These people can contact the Council of State themselves after prior complaint to the Commission. These assumptions did not apply in 2023.

Five new requests were referred to the Council of State on the basis of Article L. 8411 of the French Internal Security Code in 2023 and four decisions were issued.

As of 31 December 2023, four cases registered in 2023 remained pending.

The CNCTR is informed of any request submitted on the basis of Article L. 841-1 of the French Internal Security Code and is invited to share, where appropriate, written or oral observations. It thus has an observer status before the Council of State. As a decision-making authority, the Prime Minister, represented by the Inter-Ministerial Control Group, has the capacity to defend on behalf of the State.

The CNCTR produced observations on all the requests communicated to it by the Council of State.

As in previous years, the Commission was not in the position to itself bring a contentious appeal before the Council of State on the basis of Article L. 8338 of the French Internal Security Code. This means of appeal can only be used by the chairman of the Commission or three of its members when the Prime Minister does not respond (or insufficiently) to the opinions or recommendations of the Commission[30].

30. The Commission was also not led to submit a request to the Council of State and presented under the conditions provided for by the provisions of the second paragraph of Article L. 8211 of the French Internal Security Code as it was amended by the law of 30 July 2021.In application of these provisions, the chairman of the CNCTR or one of its members having the status of magistrate, shall immediately refer the matter to the Council of State when the Prime Minister issues an authorization for the implementation of an intelligence-gathering technique after a negative opinion issued by the Commission. The Council of State then rules within twenty-four hours of this referral. The authorization decision of the Prime Minister cannot be executed before the Council of State has ruled, except in cases of duly justified emergency and if the Prime Minister has ordered its immediate implementation. In 2023, as in previous years, the Prime Minister followed all the negative opinions issued by the CNCTR.

Improvable control methods in terms of international surveillance

Pursuant to the provisions of paragraph 4 of Article L. 854-9 of the French Internal Security Code, the CNCTR may be contacted by any person who wishes to verify that no international surveillance or spot check measure[31] is being carried out irregularly with regard to it. The Commission then ensures that any international electronic communications surveillance measures implemented comply with the applicable legal and regulatory framework as well as the decisions and authorizations of the Prime Minister.

As in the case of domestic surveillance, the Commission notifies the author of the complaint that the necessary checks have been carried out, without confirming or denying the implementation of surveillance measures or spot checks.

In 2023, only one complaint involved the verification of the regularity of the implementation of international surveillance measures.

The Commission has tools allowing it to exercise the control incumbent on it from its premises for a certain number of techniques implemented for domestic surveillance, but the same does not apply to international surveillance.

The absence of remote access to secure computer applications considerably makes control operations difficult in this matter, thus demanding that a delegation of the Commission went to each of the specialised intelligence services in order to carry out the necessary control operations, which can be long and complex.

In view of the evolution of the number of complaints submitted to it, the CNCTR considers that an improvement in the conditions of its control

31. The authorisation of the Prime Minister to exploit communications sent or received abroad or the intercepted internet connection data alone constitutes authorisation to carry out spot checks within the intercepted internet connection data for the sole purpose of detecting a threat to the fundamental interests of the Nation linked to the relationships between subscription numbers or technical IDs linked to French territory and geographical areas, organisations or individuals mentioned in 3° of III of Article L. 854-2 of the French Internal Security Code. For the sole purpose of urgently detecting a terrorist threat, this spot check may relate to communications of subscription numbers or technical identifiers linked to the national territory. Spot checks can also be implemented to detect elements of cyberattacks likely to harm the fundamental interests of the Nation on communications of technical identifiers linked to the national territory, for technical analysis purposes.

in terms of international surveillance is necessary. If this improvement can take, initially, the form of access to so-called mixed communications[32] from the Commission's premises and the provision (early 2024) of a room dedicated to the Commission with access to the data of each of the specialised intelligence services within a short period of time and without prior organisational constraints, the CNCTR considers it essential in the medium term to go further by organising access from its own premises to all information systems making it possible to control the traceability devices, the information collected, the recordings, extractions, transmissions and statements referred to in Article L. 854-9 of the French Internal Security Code as should ultimately be the case in terms of computer data collection (see point 3.1 below).

2.2. The efforts made by the divisions are still not enough to prevent the recurrence of some failures

During its ex-post controls carried out in 2023, the CNCTR noted, as in previous years, some irregularities, at each stage of the life cycle of the intelligence-gathering technique: from the implementation of a technique for exploiting the data collected both in terms of domestic surveillance and international surveillance.

If the irregularities relating to the modalities of implementation of the techniques (perimeter, field of application, etc.) are increasingly rare, they are also the most sensitive in terms of attack on individual freedoms to the extent that they have led to the collection of data that should not have been collected (2.2.1). In terms of exploitation of the technical output, the anomalies noted are, for the most part, not of a major nature; they nevertheless raise questions regarding their recurrence or persistence from one year to the next, despite the measures taken by the services to improve practices (2.2.2).

32. i.e., referring to subscription numbers or technical IDs that can be associated with the national territory.

2.2.1. The anomalies observed in the implementation phase of Intelligence-gathering techniques: few in number but high stakes in terms of public freedoms

Anomalies linked to the diversity of possibilities offered by techniques

As in previous years, the Commission noted a certain number of cases where a service, in order to install a technique, entered private property without having the required authorisation.

It happens that a service does not anticipate the necessity of having to enter private property[33], where applicable for residential use, or omits this possibility in the motivation of its request. At the investigation stage, the absence of such information may distort the proportionality control carried out by the Commission. After authorization, the control carried out ex-post may reveal an unplanned entry into a private place for residential use even though this measure is only open to a limited number of services and for a limited number of purposes.

Thus, even if this type of irregularity is now rare, it constitutes a serious attack on private life and can give rise to criminal liability for the agents responsible for the operation.

Inaccuracies or omissions in the request may also vitiate the examination of requests for the collection of computer data. Indeed, this technique, treated very concisely by the legislator, in practice covers very different operating methods whose intrusive nature can vary greatly. However, the details relating to the methods of collection envisaged by the service, the number and type of devices deployed or even the spaces and storage media used for the implementation of the technique have a direct impact on the assessment of proportionality.

33. Entry into a vehicle or private property (ILP) is provided for by the provisions of Article L. 853-3 of the French Internal Security Code. If the private property involved is a place of residence, the opinion of the Commission comes from one of its collegial bodies.

of the measurement. The services are therefore regularly invited by the Commission to further detail their requests and to explain the operational context as well as the concrete results sought by the implementation of this technique.

The Commission may be required to issue restrictive opinions so that the authorisation granted only applies to certain operating methods or even to certain media. However, in rare cases it is true, the controls carried out ex-post have been able to reveal an implementation of the technique which does not correspond to the description appearing in the request, includes unforeseen aspects or even does not comply with certain restrictions set by the Commission. These irregularities have the effect of leading to the collection of data that should not have been collected.

Anomalies arising from the overrun of the authorization period or the relevant collecting period

Less frequently than in the previous year, the CNCTR noted that some overrun of the implementation authorisation period allowed by the legal framework. In practice, these overruns could last up to ten days.

Furthermore, it noted irregularities relating to the effective implementation of the technique beyond the purpose of the surveillance. This may involve hypotheses where the service continued to operate a technique while the targeted person was not or no longer present in the planned location or carried out too extensive an implementation of the technique compared to a time-limited event. These irregular practices most often result from a technical difficulty in configuring the monitoring system or from operational constraints that do not always allow the service to intervene to limit the implementation of the technique to what is strictly necessary.

Anomalies relating to the traceability of actions carried out by intelligence services

Despite the efforts noted this year, some irregularities are still noted in terms of compliance with traceability requirements[34]. Thus, the ex-post controls carried out by The Commission were able to reveal the absence of traceability sheets, that they were drawn up too late or were even incomplete. The number of these anomalies varies depending on the type of technique implemented and the services in question. Indeed, differences in organization within services or the different methods of data collection can lead to varying delays in establishing traceability sheets and have an impact on the quality of the monitoring reported.

Thus, even if services tend to comply more and more with the requirements in this matter - the Commission regularly reminds them upstream and downstream of its controls, irregularities in terms of traceability are still noted, particularly in the case of change in systems. (in the event of breakdown, removal or exchange of the latter) or change in operational situation. They may also take the form of errors or omissions in the dates recorded, or insufficiency in the description of the devices used or even the locations of deployment.

The issue is important for the commission to the extent that only the correct establishment of these elements of traceability makes it possible to both effectively prepare the controls carried out in the services and to improve the processing of possible requests for renewal of the techniques concerned.

The commission therefore encourages the services to always show attention and rigour in establishing the traceability of the elements specific to each technique and the operational context encountered, including when a technique cannot be implemented, in particular by indicating exhaustively and precisely the actions carried out on the technical selectors added, modified or deleted.

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

2.2.2. The anomalies observed at the stage of data exploitation: less problematic in terms of infringement of public freedoms, their recurrence and persistence over the years nevertheless raise questions

More important quantitatively, these anomalies constitute attacks of less seriousness than those noted at the stage of implementation of the techniques insofar as they relate to data which the services legitimately have since they have been regularly collected. However, their recurring and persistent nature leads us to call on the services to continue their efforts in terms of training and internal control.

Irregularities noted in domestic surveillance

Overrun of the legal storage period for the raw data collected.

The French Internal Security Code provides in its Article L. 822-2, that the information collected, including when it has not been fully used, shall be destroyed before the end of a certain period, the duration of which varies depending on the nature of the data and the invasion of privacy.

In two cases in 2023, the data unduly retained came from a technique for capturing words spoken in a private capacity[35].

In the first case, it appeared that these data were kept on a server not subject to an automatic deletion script and that a lack of vigilance, admitted by the service concerned, was at the origin of this retention beyond of the legal deadline. On the recommendations of the commission, the data was quickly destroyed and this was justified by producing a report.

In the second case, although the server on which the data was hosted had a script automating the deletion, the destruction deadline was not respected because the starting point of the retention period was incorrect. The department affected by this anomaly, which had

35. See the provisions of Article L. 853-1 of the French Internal Security Code.

already been confronted with a similar problem last year and had remedied it on another of its information systems, extended the fixes to the server concerned and proceeded, in accordance with the request from the CNCTR, to the destruction of unduly retained data.

In 2022, 19 anomalies of this type were detected. These were cases where data had been collected using the computer data collection technique[36].

The CNCTR underlines in this regard that the collecting of data, among the most intrusive to private life, still escape the centralisation system organised by the Inter-Ministerial Control Group even if significant progress has been made in this area in 2023 (see part 3 of this report). As a result, compliance with the rules for conservation and use of collected data is based on the reliability and rigour of the internal procedures put in place by the services.

The Commission therefore calls for the continuation of the efforts led by the Inter-Ministerial Control Group in 2023 to put in place a partial centralisation solution limited to certain services, in particular through the development of secure computer networks allowing the routing of a significant volume of data. Concerning the "large" services currently using their own centralisation systems, the CNCTR welcomes the prospect of centralisation at the Inter-Ministerial Control Group in the medium term while respecting their operational capacities (see part 3 of this report).

However, while awaiting these developments, the CNCTR calls on all services to be extremely vigilant regarding the use of this technique, which has been increasing for four years.

Abusive transcriptions

As in 2023, the irregularity most frequently noted during ex-post controls consisted of transcriptions of elements with no link with the purpose(s) which justified the collection of information, or even, in rarer cases, with the person being monitored.

36. See the 2022 CNCTR activity report, p. 42.

In this area, the issue of protecting privacy is all the more significant since, unlike so-called "raw" data subject to restricted retention periods[37], transcriptions and extractions, which constitute "relevant" data, can be kept as long as they remain essential to the pursuit of one of the legal purposes[38].

Assessing the advisability of retaining this data can sometimes prove very delicate, while assessing the relevance of the investigation strategy adopted by the services does not fall within the prerogatives of the commission. On the other hand, it is up to the latter to assess the existence of a link between the information retained and the legal purposes. To do this, the CNCTR carries out a more targeted but also more in-depth control[39] than that carried out systematically by the Inter-Ministerial Control Group's control office on the techniques subject to centralisation[40].

This control is carried out both for the examination of requests for renewal of a technique and in the perspective of documentary audits and on-the-spot inspections. These verifications can be carried out spontaneously, at the initiative of a project manager or the ex-post control centre, or on a scheduled basis, with certain opinions conditioning the renewal of an authorisation on the monitoring of the results of the exploitation of the technique considered.

When a question arises as to the relevance of the elements appearing in one or more transcriptions, an exchange is established with the service[41] in order to determine whether the production(s) shall be destroyed or can, on the contrary, be preserved.

37. See Article L. 822-2 of the French Internal Security Code

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

39. This control is carried out using secure computer applications made available to the commission by the Inter-Ministerial Control Group which allow it to access, at any time, directly from its premises, all of the transcriptions made from security interceptions as well as 'to those resulting from speech and image capture techniques which are centralized.

40. Before being made available to the agents of the service concerned, any transcription or extraction project is subject to validation by the Inter-Ministerial Control Group control office which ensures that the information contained therein relates to the target designated in the authorisation. intelligence-gathering technique and that the traceability of this exploitation is correctly fulfilled. In addition, a check is carried out on the adequacy between the very content of the "production" and the object of surveillance.
When the Inter-Ministerial Control Group identifies a difficulty, it initiates a dialogue with the service which may result in the validation and dissemination of the "production" or, conversely, the deletion of the disputed content.

41. See (c) of this part below.

In 2023, all productions for which the CNCTR confirmed its request for destruction following dialogue with the service were destroyed within a satisfactory time frame.

As part of this reinforced control, the CNCTR pays particular attention to transcriptions and extractions from authorised intelligence-gathering techniques with regard to people exercising a so-called "protected" profession or mandate[42]. Indeed, the provisions of Article L. 821-7 of the French Internal Security Code prevent these people from being the subject of a surveillance measure due to their profession or mandate[43].

Among the anomalies observed in 2023, two were noted as part of the surveillance of these protected professions. Thus, the commission noted that the services had transcribed elements concerning them which were directly linked to their profession.

These irregularities gave rise to requests for destruction of the data thus capitalized to which the services concerned quickly responded..

In one case, an on-the-spot inspection and documentary audit revealed that a department had kept data which, although relevant to the purpose pursued at the time of their collection, related to investigations which had already allowed us to finally rule out any link with this purpose. In practice, the anomaly noted did not result from a deliberate desire to circumvent the legal framework but from a misunderstanding of its scope in such a configuration. This applicable legal framework was recalled and clarified by the commission and the disputed data was destroyed by the service concerned.

Persistent difficulties in establishing information bulletins reporting actions to exploit the data collected

Article L. 822-4 of the French Internal Security Code provides that transcriptions and extractions are the subject of records kept at the disposal

42. These are parliamentarians, lawyers, magistrates and journalists.

43. Article L. 854-3 of the French Internal Security Code provides similar protection in the context of the surveillance of the international electronic communications of these individuals when the latter exercise their profession or mandate on the national territory. See on this point the study appearing in the 7th 2022 CNCTR activity report, p.93 and following

of the Commission, the law also guaranteeing its permanent, complete and direct access to the records, registers, information collected, transcriptions and extractions.

On several occasions in 2023, the Commission noticed that transcriptions or extractions had not given rise to any information bulletin or had not been centralised by the service so that they were inaccessible to the Commission and, therefore, escaped its control while these bulletins are meant to capitalise on the relevant information which will be retained.

These irregularities reveal that, despite the development of information systems dedicated to the exploitation of data resulting from the implementation of intelligence-gathering techniques, there are still many agents who persist in working on their own non-centralised files, from their own workstation, without any traceability.

Already drawn up in 2022, this observation, worrying in that it highlights a risk of poorly or even uncontrolled dispersion of the data collected, led the Commission to initiate a dialogue with the entities responsible for internal control within the services involved. If progress had then been recorded both with regard to the deadlines for establishing the information bulletins and their completeness, it is clear that they were not sufficiently pursued at the end of 2023 and that the difficulty is recurring in certain services.

The CNCTR therefore calls for constant vigilance and renewed efforts by internal control services in order to sustainably resolve these difficulties.

Irregularities observed in the surveillance of international electronic communications

As with domestic surveillance, the CNCTR regularly carries out checks on data resulting from the surveillance of international electronic communications, whether it concerns the conditions of their collection, their conservation or their exploitation.

While until October 2023 it had no access to data or traces of research carried out by service agents, the CNCTR is now equipped with two computer workstations allowing it to access transcriptions of so-called mixed communications (that is to say referring in part to subscription numbers or technical identifiers linked to the national territory).

The result of consultation work carried out between the CNCTR, the Inter-Ministerial Control Group and the General Directorate of External Security, the provision of this equipment constitutes significant progress in the control of international surveillance, allowing the commission to now have direct access to the information collected.

During 2023, irregularities of the same nature as those recorded in 2022 were noted during the various controls carried out by the CNCTR in the field of international electronic communications monitoring.

Data exploitation carried out in disregard of legal provisions

Under Article L. 854-1 of the French Internal Security Code, surveillance measures for international electronic communications shall comply with the general principle according to which international surveillance does not allow, except for exceptions expressly provided for by law, to intercept national communications.

On several occasions in 2023, the CNCTR noted that services had carried out, outside of legal exceptions, questionings on technical IDs linked to the national territory which were in communication with a person located on French soil.

Furthermore, while the transcription of a communication intercepted in the context of international surveillance presupposes, by virtue of the principle recalled above, that at least part of this communication presents a foreign criterion, the commission has, in several services, found that transcripts reported communications occurring between two people located on national territory at the time of the interception.

The CNCTR also discovered on three occasions that the exploitation of communications exceeded the scope of authorizations issued by the Prime Minister. From the commission's point of view, these irregularities, although quantitatively limited, constitute very serious breaches.

It was finally noted that an agent had, without authorization, carried out searches in a data storage space benefiting of specific protection without it being possible to determine, on the one hand, whether the requests made related to connection data[44] or content, on the other whether they had allowed the operator to actually access to this data.

Consultations or operations not related to the relevant authorization

Just like last year, the most frequently noted anomalies but also the most benign consist of the consultation or use of data that the agent does not link to the relevant authorization.

The exploitation of data resulting from the surveillance of international electronic communications is carried out by specialized agents, using specific computer applications whose rights and material conditions of access are strictly limited and controlled. This exploitation consists, for the agents concerned, of querying the bases housing the data by formulating a "query" based on the exploitation authorization granted to the service.

The CNCTR therefore verifies that the elements sought are actually linked to the object of the authorized surveillance measure, whether the targets monitored or the legal purposes pursued.

This year again, the commission regularly noted that consultations and even use of data had been electronically linked to irrelevant authorizations.

It appears from the explanations provided by the services that negligence on the part of the operating agents or errors in handling the IT tool[45] are at the origin of these anomalies.

44. In such a scenario, this request could fall under the regime of spot checks (see below) and not constitute an irregularity.

45. The IT tool assists the user by automatically offering them, with each new request, the operating authorization invoked for the previous request.

Despite the training actions for agents carrying out the exploitation of international surveillance and although in decline, the frequency of these anomalies remains at a level which must, from the point of view of the commission, encourage the services to continue these training actions which, combined with regular reminders carried out by the legal departments and offices concerned, must result in lastingly curbing these irregularities.

Irregularities in spot checks

Other irregularities have also been noted in the practice of "spot checks". Provided for by Title IV of Article L. 854-2 of the French Internal Security Code, these spot checks make it possible to deviate from the principle banning the use of international surveillance measures to intercept national communications. They make it possible to detect, within the connection data, a threat to the fundamental interests of the Nation linked to the relationships between subscription numbers or technical identifiers linked to the national territory and geographical areas, organizations or people making the connection. subject to surveillance.

In two hypotheses, these legal provisions also provide that these verifications can be carried out on so-called "content" data, which are inherently more intrusive to privacy. This involves, on the one hand, urgently detecting a terrorist threat. The numbers and identifiers must then be immediately communicated to the Prime Minister and the CNCTR for control purposes. This is, on the other hand, to enable the detection of elements of cyber-attack likely to undermine national independence, territorial integrity or national defence.

Research carried out in this context cannot exceed a certain duration. However, the commission found again this year that this condition had not been respected and that spot checks on communications had been carried out outside of legal requirements.

2.2.3. The course of actions further to detecting irregularities and anomalies: divisions willing to correct them; future verifications sometimes required, and progress to be made to prevent them from happening again

When an ex-post control leads to the discovery of an anomaly or irregularity, the CNCTR implements a procedure established for several years and producing, in its opinion, satisfactory results.

Thus, the department concerned is systematically informed so that a contradictory exchange can be initiated. The discussion begins informally during the inspection and continues with a written notification sent by secure means to the service inviting it to submit its observations.

Just as in 2022, all the findings and analyses drawn up by the Commission this year were shared by the services which ensured that an end was put to them within a short period of time, without the Commission having to use the power of formal recommendation conferred by Article L. 833-6 of the French Internal Security Code.

The CNCTR thus ensured that all illegally stored raw data had been destroyed and had not given rise to any exploitation.

Regarding transcriptions and extractions, the dialogue initiated with the services systematically resulted in a jointly accepted solution. Thus, depending on the case, these exchanges led to the justification of their conservation with regard to the elements provided by the service or, on the contrary, to the confirmation of the request for destruction. In this second hypothesis, the commission requests the communication of the destruction reports and can, if necessary, carry out checks within the information systems in which the data are stored.

If the requested destructions take place within a time frame deemed satisfactory by the commission, its verifications have several times revealed that the ad hoc reports sent to it were erroneous, or that

they did not mention all of the data or transcriptions and extractions destroyed, or because they were incorrectly or incompletely referenced.

The CNCTR attaches great importance to the quality of the drafting of these minutes and encourages the services to take the greatest care. In fact, these acts constitute a formal commitment by which the service attests to the reality of the destruction of raw data unduly preserved or of transcriptions and extractions that are irregular or have become irrelevant. The sincerity and accuracy of the information given in these minutes therefore appear essential.

Beyond simply noting anomalies and irregularities, the commission endeavours to precisely identify the stage(s) of the internal processes during which the irregularities occurred in order to consider, in consultation with the department concerned, the adjustments and corrective measures to be taken bring in order to prevent any reiteration.

Its mission is not limited to correcting past irregularities. It also consists of ensuring, for the future, the absence of renewal. To achieve this, it supports and, in certain cases, guides the implementation of good practices within services to ensure full compliance with the legal framework.

The irregularities and anomalies detected in 2023 did not reveal any deliberate desire to conceal or circumvent the legal framework.

However, they demonstrate persistent difficulties in appropriating good practices by certain agents of the intelligence services. For several years, legal services have undertaken actions to disseminate and explain the framework for using the techniques information for each actor involved in their life cycle. Although the commission calls for the continuation of these steps, progress still remains to be made. In particular, internal procedures intended to centralize the exploitation of techniques in information systems accessible to the commission are still not correctly applied.

Furthermore, the repetition from one year to the next of anomalies, even of low severity, testifies to the persistence of elementary errors resulting from the non-integration, into daily working methods, of reminders and recommendations from the commission which are only followed by effects piecemeal.

More than eight years after the entry into force of the law of 24 July 2015, the Commission notes that the same anomalies and irregularities persist from one year to the next. This situation shows that the preventive measures deployed by the services are insufficiently effective. This observation is worrying in a context of a significant increase in the volume of data collected using intelligence-gathering techniques that are particularly detrimental to privacy and the increasing complexity of the systems used to process it.

Also, the CNCTR considers that, to guarantee an acceptable level of efficiency and reliability of its ex-post control and in the face of the challenges posed in particular by the growth in the collection of computer data, the modalities for exercising this control shall necessarily evolve towards remote access (see part 3 of this report).

Section 3. Areas of vigilance and prospects for the years to come

3.1. Collection of computer data: continuing to improve control[46]

3.1.1. The specific challenge of the technique used to collect computer data in the commission's ex-post control task

The Commission wishes to emphasize, in this 2023 report, the issue of ex-post controls of computer data collected following the implementation of authorised intelligence-gathering techniques. However, it has not excluded from its areas of effort the ex-ante control of requests for this implementation. Where necessary, it has decided to combine its favourable opinions with restrictions intended to regulate data collection capacities in order to better ensure respect for the principle of proportionality and protect individual freedoms.

Such restrictive opinions would risk being devoid of scope if the commission did not have, downstream, the technical knowledge and monitoring capabilities, on-the-spot or remotely, sufficient to enable it to verify their correct application. In this regard, 2023 was a rich year.

As the commission emphasized, this progress was necessary to ensure effective control of a technique with strong particularities.

46. The technique of collecting computer data is mentioned in Article L. 853-2 of the French Internal Security Code which provides in particular that: "*Under the conditions provided for in Chapter I of Title II of this book, when the information cannot be collected by another legally authorized means, the use of technical devices allowing access to computer data stored in a computer system, to record, store and transmit them, and allowing access to these same computer data, to record, store and transmit them, as they are displayed on a screen for The user of an automated data processing system, as he enters it by entering characters or as it is received and transmitted by peripherals.*"

These are not limited to the volume of data collected, which is incommensurate with what security interception allows.

Indeed, unlike other intelligence-gathering techniques for which the nature of the elements collected is inherent to the technique implemented (the use of a tag, for example, is only likely to lead to the provision of location data), the collection of computer data covers various modalities of action, can take the form of multiple technical devices and result in very varied data collections both in terms of their scale and their nature or quality.

Furthermore, unlike the intelligence-gathering techniques centralised at the Inter-Ministerial Control Group which are, in fact, relatively standardised, the practice of collecting computer data can significantly differ depending on the service that uses it, the type objective concerned[47] or even the operational circumstances.

Thus, beyond the very general definition of technique given by law in Article L. 853-2 of the French Internal Security Code, the precise technical modalities for implementing computer data collections depend on multiple factors: the type of information sought, the nature and characteristics of the targeted equipment, the operational conditions and opportunities for implementation, the devices used or even the operating methods specific to the user service.

For example, the means to be implemented to collect data are necessarily different and have a more or less intrusive nature depending on whether they are contained in a removable storage medium belonging to the targeted person or within a network of machines compromised by a group of foreign hackers.

This heterogeneity of the technique is also found at the stage of exploitation of the data collected. The type of support used, the tools implemented for this exploitation and the practical operating methods

47. The objective designates, within the meaning of 6° of Article L. 821-2 of the French Internal Security Code, "the person(s), place(s) or vehicles concerned".

specific to a service lead to large differences at the capitalisation stage both in the nature and in the volume of data involved, in particular with regard to extractions[48].

Thus, in the event of a cyber-attack mentioned above, intelligence services face significant variability and high complexity of the operating methods to detect and the traces on which to carry out intelligence investigations. The work of capitalizing the service can then be sequential, by multiple professions, on supports and networks with various functionalities. This complexity is added to the multiplicity of types of data collected and volumes generated by the use of the computer data collection technique. This results in a particularly difficult control for the CNCTR, including understanding the service's approach and sometimes assessing the link with the stated purpose.

3.1.2. 2023 saw great progress being made to make the control more effective. Some remain to be realized.

The continuation of a constructive dialogue with the services and the support of the National Coordination of Intelligence and the Fight against Terrorism (CNRLT) made it possible over the past year to ratify significant progress and to stop the at this stage the risk of a weakening of control. Three projects are notable in this regard.

Removing certain "blind spots"

Firstly, the technical dialogue established with the services led to the removal of several "blind spots" in the commission's ex-post control. Access to information has thus improved regarding the two services which jointly represent the majority of the data collected, allowing the commission to have a broader vision of the collection and exploitation conditions used.

48. Legal mechanism allowing the capitalization of raw data specially selected for their link with the purposes and reasons targeted by the authorization.

The transmission of technical statistics allows the CNCTR to obtain an updated status of the implementation of authorized collections and to measure the volume of data collected upstream of any capitalization by the service. This acceleration of the provision of information, authorising the commission to anticipate its documentary audits and on-the-spot inspections, allows it to better target its intervention.

Furthermore, the content of the traceability elements to be established by the service has been adjusted. While preserving the confidentiality of the operational terms of the services, the additional description elements provided make it possible to improve the CNCTR's ability to analyse and interpret the operations carried out and the information collected. They facilitate the verification of the correlation between the motivation provided by the service in support of its request and the reality of the action it carried out in the field once the technique was authorized.

Finally, with regard to one of the first-line services, the carrying out of technical developments in its internal information system allowed the granting to the Commission of a single point of access to examine all the stored data locally, thus speeding up the exercise of documentary audits and on-the-spot inspections. Beyond that, the approach taken by the department concerned made it possible to secure data management and the application of destruction deadlines, in particular by limiting the making of manual copies and the use of external media.

The Commission therefore welcomes the strengthening of this technical dialogue with the services, which it called for at the end of 2022, and the concrete progress that it has enabled during the year 2023.

A new tool allowing centralized operation for a still limited field

A new possibility of centralising the data collected was opened by the Inter-Ministerial Control Group in 2023. It does not call into question the conservation of data performed by the two major user services but it offers other services which use RDI, more or less frequently, a centralized operating tool for certain collection methods.

Like the information system set up for security interceptions, this tool, which is intended to evolve, offers a secure framework for the integration of data, their manipulation and the carrying out of transcription and dissemination operations. data extractions. The CNCTR benefits directly from this work which allows it immediate access to the data collected. Thus, a computer station directly connected to this specific network has been installed since the end of 2023 in the Commission's premises.

If improvements are expected to allow the implementation of more sophisticated and more fluid operating tools for the work of service agents, the commission welcomes this progress, which also contributes to the pooling of technical capacities between the services. However, it only affects a very small part of the RDI carried out.

In the longer term, an ambitious project to centralize all RDI techniques guaranteeing the commission direct access to all the data collected

The Commission's activity report for the year 2022 highlighted the difficulty in controlling the use of RDI and the resulting risk of "dropping out" of control. Aware of this risk, the President of the Republic asked the National Coordinator of Intelligence and the Fight against Terrorism (CNRLT) to encourage joint reflection between the two services mainly concerned (the General Directorate for Internal Security, DGSI, and the Directorate General for External Security, DGSE) on an evolution of control possibilities.

The project finally decided consists of bringing together all of the data collected on the Inter-Ministerial Control Group systems. The commission will thus be able to access it remotely under guaranteed security conditions. The services themselves will be able to use the data collected also remotely. Their operating conditions, not only will not be degraded, but they will even be improved because this "virtual Inter-Ministerial Control Group " will also make available the data collected by traditional telephone tapping that the services could until now only exploit by travelling physically in the Inter-Ministerial Control Group premises.

The first feasibility studies will start in the second half of 2024 with a goal of commissioning the new tools in the course of 2027.

Pending the completion of this project, which is essential to the effectiveness of the mission entrusted to the commission, the regular technical dialogue initiated with the services will be continued to prevent any loss of control.

3.2. A law-making meeting in 2025, which will be an opportunity to bring about progress in the legal framework towards increased compliance with European requirements and improved consistency and effectiveness

Law No. 2021-998 of 30 July 2021 relating to the prevention of acts of terrorism and intelligence, known as the PATR law, introduced into the French Internal Security Code a new Article L. 852-3 allowing, under the purposes mentioned in 1°, 2°, 4° and 6° of its Article L. 811-3, to use a device or technical equipment in order to intercept correspondence sent or received by satellite, "when this interception cannot be implemented on the basis of I of Article L. 852-1", that is to say when the use of telephone tapping is not possible for operational or confidentiality reasons.

Article 13 of the law of 30 July 2021 provides that these provisions will be applicable until 31 July 2025 and that the Government provides Parliament with an evaluation report on the application of these provisions no later than six months before this due date.

In the absence of setting the maximum number of satellite interception authorisations that can be granted simultaneously, this new technique was not implemented during 2023. It should be in 2024, leaving limited time to take stock of it in accordance with the request of the law-maker.

New legislative intervention is therefore expected during 2025, at least to clarify the future of this technique. However, ten years after the intervention of the laws of 24 July 2015 and 30 November 2015, this legislative meeting constitutes an opportunity to evolve the provisions of the French Internal Security Code both in order to better meet the requirements of the jurisprudence of the European Court of Human Rights (ECHR) in a context where decisions should finally be taken on the various requests, relating to the law of 24 July 2015, targeting France (3.2.1) but also in order to improve the internal coherence and effectiveness of the regime then adopted (3.2.2).

3.2.1. A change in the legal framework seems to be necessary in light of the requirements of the European case law, in particular with regard to exchanges with foreign organisations and so-called sovereignty files while several court decisions regarding France are expected to be issued in 2024

As the Commission has had the opportunity to mention on several occasions in its previous reports[49], fourteen applications submitted to the ECHR between 7 October 2015 and 21 April 2017 and relating to the provisions of the French Internal Security Code resulting from the law of 24 July 2015 are currently still pending. The decisions, first announced for 2022 then for 2023, have not yet been made as of the printing date of this report but should be in the coming weeks.

For the record, some claimants argue that the intelligence-gathering techniques provided for by law do not meet the requirements of a sufficient legal basis. They thus believe that the notion of "information or documents" that can be collected by means of an intelligence-gathering technique is not defined and that the law does not sufficiently

49. See in particular points 1.2.2 of the 6th 2021 activity report and point 3.2.1 of the 7th 2022 activity report, available on the CNCTR website.

protect people who are either journalists or lawyers. They further consider that the legislator has retained a broad definition of the legal purposes which may underlie the implementation of surveillance measures, the legal regime thus created not being, according to them, "strictly necessary for the preservation of democratic institutions".

Furthermore, the claimants complain of insufficient procedural guarantees. They thus allege a lack of effective recourse in that, on the one hand, the appeal before the CNCTR and the Council of State would not meet the requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms (lack of recognition of the principles of equity, adversarial matters and equality of arms), on the other hand, that it is impossible to directly refer international surveillance measures or the collection and use of information coming from foreign services to the Council of State.

However, in light of the Court's previously established jurisprudence in matters of intelligence, a change in the French legal framework appears inevitable.

Indeed, the judgements handed down by the Grand Chamber of the Court on 25 May 2021 (Big Brother Watch and others v. United Kingdom[50] and Centrum för rättvisa v. Sweden[51]) relating to the British and Swedish surveillance regimes led, on the one hand, to remember that the devices for mass interception of electronic communications likely to be put in place by the States parties shall provide "end-to-end guarantees" and to specify these guarantees[52]. Among these are the organization of supervision by an independent authority of compliance with the guarantees set out and the establishment of independent ex-post control as

50. See ECHR, 25 May 2021, Big Brother Watch and others v. United Kingdom, No. 58170/13.

51. See ECHR, 25 May 2021, Centrum för rättvisa v. Sweden, No. 35252/08.

52. The Court seeks in particular whether the national legal framework defines sufficiently clearly: the grounds on which mass interception may be authorized; the circumstances under which an individual's communications may be intercepted; the procedure for granting an authorization; the procedures to be followed for the selection, examination and use of intercepted material; the precautions to be taken when communicating these elements to other parties; the limits placed on the duration of interception and retention of intercepted material, and the circumstances in which such material must be erased or destroyed; the procedures and arrangements for supervision, by an independent authority, of compliance with the guarantees set out above, and the powers of this authority in the event of a breach; and the procedures for independent ex-post monitoring of compliance with guarantees and the powers conferred on the competent body to deal with cases of breach.

well as the granting of sufficient powers to the competent body to deal with possible shortcomings. On the other hand, the Court considered that if the international sharing of data between foreign intelligence services could be accepted, it must be governed by predictable and accessible rules, present guarantees in the management of the data concerned and be subject to an independent control.

Thus, with regard to these exchanges with foreign services, new rules should be set in the French Internal Security Code to limit outgoing flows (information likely to be transmitted to a foreign service) to data collected in accordance with the provisions of its book VIII, the recipient States must provide sufficient guarantees in terms of use, conservation and non-disclosure of data[53]. Regarding incoming flows (information received from foreign partners), these rules should at least prohibit the receipt of data the collection of which would have been prohibited by French law. Furthermore, the existence of supervision of exchanges by an independent authority would be necessary at least when they take place with a State which is not a party to the European Convention for the Protection of Human Rights and Fundamental Freedoms[54].

With regard to so-called sovereignty files, the control currently entrusted to the Commission by the provisions of the French Internal Security Code cannot be considered exhaustive in the absence of access to all the data storage spaces of the services within from which it would be possible to conceal information excluded from the scope of its competence[55]. Furthermore, only such access is likely to allow it to fully exercise its control when it receives a complaint on the basis of Article L. 833-4 or Article L. 854-9 of the code it being emphasized that the answers provided to the complainants cannot lead to the revelation of information covered by national defence secrecy. In this regard, the legal framework control

53. The Court holds that it is up to a transmitting State to ensure that the organization or State receiving the data has put in place rules to guarantee that the processing of this data will not be subject to abuse. disproportionate or interference, without however requiring that this receiving State presents guarantees strictly identical to those presented by the transmitting State.

54. As it stands, the provisions of 4° of Article L. 833-2 of the French Internal Security Code do not allow the CNCTR to require access to "elements communicated by foreign services or by international organisations".

55. The provisions of 4° of Article L. 833-2 of the French Internal Security Code do not in particular allow the CNCTR to require access to elements which could give it knowledge "either directly or indirectly of the identity of the sources of the specialised intelligence services".

entities set up within the services, even if the members of this internal structure benefit from a particular status allowing them to have a certain autonomy, do not make it possible to respond to the requirements set by the ECHR which provide that the control must be independent of the authorities carrying out the surveillance.

Finally, with regard to the terms of the right to appeal and more particularly the principle of the contradictory nature of the procedure, better compliance with European requirements could involve an improvement of the current system which does not allow either the claimant or his counsel to have knowledge of all the elements accessed by the Council of State. In this regard, like the British model of "secret evidence" made accessible only to lawyers specially authorised[56], it could be envisaged the creation of a pool of lawyers authorised for national defence secrecy to whom the claimants could call for their defence without being able to themselves access information relating to such secrecy.

The legislative meeting scheduled for 2025, which should take place after the Court's decisions concerning France, is an opportunity to evolve the French legal framework towards better respect for the guarantees set out by the Court's case law. Beyond that, it could help improve the coherence and efficiency of the current legal framework on various points.

3.2.2. Developments would also be useful to improve the coherence and efficiency of the current legal framework.

After nearly ten years of application of the 2015 laws, it appears that certain techniques which had caused a lot of concern are proving to be less detrimental to public freedoms than other techniques which had nevertheless caused less debate. As a result, a stricter quota or framework has sometimes been provided for less intrusive techniques than others for which such a quota or framework has not been provided for by law.

56. The specially authorized lawyer can access secret evidence but cannot reveal its content to his client.

Thus, the provisions of II of Article L. 851-2 of the French Internal Security Code provide for a quota of access to technical connection data in real time and limit this technique to the prevention of terrorism while the collection of computer data provided for in Article L. 853-2 of the said code, which nevertheless allows access to a very large quantity of data, where applicable, according to very intrusive terms[57/58], is not limited and accessible for all the purposes mentioned in Article L. 811-3. Beyond that, the absence of the possibility of using real-time access to data for certain purposes, such as the prevention of collective violence, leads to the need to consider more quickly the use of more intrusive techniques.

Following the same logic, the provisions relating to international surveillance provide a very specific framework for measures likely to target identifiers attachable to the national territory (IRTN). However, the absence of a legal definition of the concept and its ambivalence, as well as the silence of the law regarding the treatment of identifiers not linked to the national territory can paradoxically lead to reinforced protection of the latter whereas such did not seem to be the intention of the law-maker of the law of 20 November 2015[59].

Furthermore, in order to clarify the scope of certain provisions, to secure the intervention of intelligence services but also to reinforce the guarantees provided to citizens, certain other notions deserve to be better clarified.

Thus, for the reasons presented in the context of the study appearing in this report[60], the concept of entourage, initially introduced in Article L. 852-1 of the French Internal Security Code, could be more explicit without reference to the any surveillance implemented with regard to the main target.

Likewise, in terms of complaints and appeals, the provisions of Articles L. 833-4 and L. 841-1 of the French Internal Security Code would require clarification regarding the extent of the checks to be carried out over time.

57. See point 3.1 above.

58. Likewise, the image or sound recording techniques provided for in Article L. 853-1 of the French Internal Security Code are not subject to a quota.

59. See in particular the provisions relating to spot checks provided for in Article L. 854-2 of the French Internal Security Code.

60. See point 2 above.

Indeed, as it stands, the Commission carries out trace checks going back to the date of entry into force of the law of 24 July 2015 regarding domestic surveillance but the time elapsed since the intervention of this law should lead us to question the advisability of setting a limit in this area. Furthermore, while the provisions of II of Article L. 822-2 of the French Internal Security Code provide that information relating to a request submitted to the Council of State cannot be destroyed and shall be kept for the sole needs of the procedure before this court, equivalent provisions are not provided for with regard to complaints addressed to the CNCTR under Article L. 833-4 or Article L. 854-9 of the said code, so that between the intervention of such a complaint, the response from the Commission and a possible referral to the Council of State of the data could have been deleted.

Finally, certain developments would be useful in order to make the intervention of the commission more fluid or more effective.

Thus, for example, the combination of the provisions of Articles L. 831-2[61] and the second paragraph of Article L. 832-3[62] leads as it stands to imposing the quorum conditions of the plenary session on requests relating in practice to the competence of the restricted body as long as at least one parliamentary member is present.

Also, requests for entry into a private place for residential use for the purposes of removal or maintenance of a device already authorized by the college training must be examined either by this same training, or by a single member having the status of magistrate. However, in the latter case, the plenary collegial formation must be informed. This information could be deleted or, at the very least, could be brought before the restricted collegial panel.

61. "The plenary body of the National Oversight Commission for Intelligence-Gathering Techniques includes all of the members mentioned in Article L. 831-1. */ The restricted body of the National Oversight Commission for Intelligence-Gathering Techniques is made up of the members mentioned in 2° to 4° of said Article L. 831-1. / (...)*"

62. "*(...)* The restricted body and the plenary body can only validly deliberate if, respectively, at least three and four members are present. *(...)*".

According to the same logic, but without any additional concrete impact on public freedoms, certain rules for the use of techniques or the supervision of the latter deserve to be harmonized for the sake of consistency and effectiveness.

This applies in particular to the duration of authorisation for entry into private property (ILP), set at 30 days by III of Article L. 853-3 of the French Internal Security Code by way of derogation from the provisions of Article L. 821-4 of the said code. ILP does not in fact constitute a technique as such, but the support necessary for the implementation of another technique such as the capture of images or sounds or the collection of computer data. However, the authorisation periods for these techniques are longer than that provided for the ILP (two months maximum under II respectively of Article L. 853-1 and Article L. 853-2 of the French Internal Security Code), so that it regularly happens that a request for renewal of ILP is necessary in order to allow the implementation of a technique that is otherwise still authorised but which, in practice, could not be installed.

In the same sense, the formulation of the quota provided for in article L. 851-6 of the French Internal Security Code regarding devices or devices allowing the identification of terminal equipment or the subscription number of its user as well as data relating to the location of terminal equipment used (IMSI-catcher) could be revised in order to target the number of authorisations granted simultaneously and not the number of devices that can be used simultaneously, which in practice makes the Commission's control over compliance with this quota very difficult or even impossible.

Studies: The grey areas of monitoring

Study 1. Outline and challenges of monitoring in the field of the prevention of organised crime

Study 2. Should the people in close contact with monitored individuals be under surveillance?

Study 1. Outline and challenges of monitoring in the field of the prevention of organised crime

The French Internal Security Code provides that the use of intelligence-gathering techniques can only be authorised for the defence or promotion of a limited number of fundamental interests of the Nation. These fundamental interests are listed in Article L. 811-3 of the Code, which distinguishes seven purposes[1] among which in 6): "*The prevention of organised crime and delinquency*".

This purpose, the scope of which was defined in reference to criminal offences justifying the use of a procedure and investigative techniques deviating from common law, therefore presents a specificity due to the fact that administrative monitoring techniques, if they are productive, shall result in referral to the judicial authority, so that the question of the articulation between administrative and judicial procedures is particularly, even necessarily, raised.

The notion of "organised crime and delinquency" within the meaning of this purpose does not, however, cover all of the offences aggravated by the circumstance of an organised gang within the meaning of the French Criminal Code, nor all of the offences likely to fall within the scope of the procedure applicable to crime and delinquency organised as per the French Criminal Procedure Code. The CNCTR, in the light of the jurisprudence of the Constitutional Council, was therefore led to specify its scope (1).

1. The other purpose listed in Article L. 811-3 include: 1) national independence, territorial integrity and national defence; 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; 3) the major economic, industrial and scientific interests of France; 4) the prevention of terrorism; 5) the prevention of: a) damage to the republican form of the institutions; b) actions aimed at maintaining or rebuilding dissolved groups pursuant to Article L. 212-1; c) collective violence likely to seriously harm public peace; and 7) prevention of the proliferation of weapons of mass destruction.

Furthermore, this purpose is more particularly likely to raise difficulties in terms of respecting the respective fields of intervention of the administrative police and the judicial authority. Through its opinions on requests for intelligence-gathering techniques, the Commission was also led to more precisely delimit the field of intervention of administrative intelligence. In this regard, it strives to promote dialogue between the intelligence services and the judicial authority in order to improve the connection between administrative and judicial procedures (2).

1. A purpose with a different scope from the meaning of the notion of delinquency and organized crime within the meaning of criminal law

The concept of organised crime was originally defined in the French Criminal Code. It led to the provision of adaptations to the common law criminal procedure (1.1). However, the purpose of the prevention of organised crime within the meaning of the French Internal Security Code covers a more restricted scope that the CNCTR has clarified following the interpretations given by the Constitutional Council in its decision no. 2015 -713 DC of 23 July 2015 pertaining to the law relating to intelligence (1.2)..

1.1. The concept of organised crime as per the French Criminal Code has several acceptations.

In the sense of criminal law and criminal procedure, organised crime can be considered similar to offences committed by an organised gang (1.1.1), but also to those for which the legislator has provided a procedural regime dispensing from common law (1.1 .2) or the jurisdiction of specialised courts (1.1.3).

1.1.1. The concept of organised gang within the spirit of French criminal law

In criminal law, the notion of an organized gang corresponds to an aggravating circumstance, which must be provided for by law and which results in an increase in the quantum of the penalty incurred. The aggravating circumstance of commission by an organized gang does not exist for all criminal offences.

Article 132-71 of the French Criminal Code provides that: "An organized gang within the meaning of the law constitutes any group formed or any agreement established with a view to the preparation, characterized by one or more material facts, of one or more offences." This definition is identical to that of the criminal conspiracy offence[2].

However, it follows from the jurisprudence of the Constitutional Council that the organised gang implies premeditation and a structured organisation[3]. The Court of Cassation also clarified that the notion of an organised gang implied logistics and a distribution of tasks between its members[4].

2. See the provisions of Article L. 450-1 of the French Criminal Code.
3. See decision no. 2004-492 DC of 2 March 2004 recital 13
4. See Criminal Cass., 8 July 2015, no. 14-88-329, Criminal journal, no. 834

1.1.2. The exceptional procedural regimes applicable to certain offences relating to delinquency and organized crime

Law No. 2004-204 of 9 March 2004 adapting justice to developments in organised crime, known as "Perben II", created a procedural regime derogating from common law for certain offences, with the aim of fighting more effectively against trafficking and organised crime. Title XXV of Book IV of the French Criminal Procedure Code thus establishes specific rules of jurisdiction, with the creation of specialized courts, and of procedure, allowing exceptions to the rules of common law applicable to police custody, searches and measures conservatories in particular. It also authorizes the use of "special investigative techniques".

In its Article 706-73, the French criminal procedure code lists the offences which allow the application of all of these rules derogating from common law. Thus, these offences are likely to justify in particular the use, from the preliminary investigation stage, of interception of correspondence, the capture of images or words in private places, an IMSI-catcher or even the capture of computer data, or techniques similar or comparable to certain techniques provided for by the French Internal Security Code for administrative intelligence.

The offences covered by this article fall, according to the circular[5] presenting the provisions of the law of 9 March 2004, into "serious organised delinquency". If some of these offences must be committed with the aggravating circumstance of organized gang to fall within the scope of Article 706-73, such as the crime of murder[6], this is not the case for others, such as crimes and offences of drug trafficking[7], crimes and aggravated offences of human trafficking human rights[8] or even aggravated crimes and offences of aggravated pimping[9], which intrinsically involve a notion of criminal organisation.

5. See in particular the circular of 2 September 2004 presenting the provisions relating to organised crime of Law No. 2004-204 of 9 March 2004 adapting justice to developments in crime.

6. See the provisions of Article L. 706-73 (1) of the French Criminal Code.

7. See the provisions of Article L. 706-73 (3) of the French Criminal Code.

8. See the provisions of Article L. 706-73 (5) of the French Criminal Code.

9. See the provisions of Article L. 706-73 (6) of the French Criminal Code.

Article 706-73-1 of the French criminal procedure code lists the offences, mainly economic and financial (notably the offences of fraud or concealment of activities or employees in an organised gang[10], or even trafficking offences of cultural property[11]), which, falling within the scope of organised crime, allow the application of all the rules derogating from common law with the exception of those governing police custody[12]. This article was introduced into the French criminal procedure code by Law no. 2015-993 of 17 August 2015 adapting criminal procedure to European Union law, following a decision of the Constitutional Council having ruled otherwise to the Constitution 8° bis of Article 706-73 of the French criminal procedure code which targeted organised gang fraud[13]. The Constitutional Council considered that this offence was not likely to "to endanger security, dignity or life in itself of persons", the exceptional regime of police custody provided for by the legislator constituted a disproportionate attack on individual freedom and the rights of the defence in relation to the aim pursued.

Offences which are not cited either by Article 706-73 or by Article 706-73-1 of the French criminal procedure code and which are committed in organised gangs fall under the regime provided for by Article 706-74 of the said code. With regard to these offences, the scope of the rules derogating from common law is much more restricted since only two special investigation techniques are applicable: the extension of the competence of officers and, where applicable, judicial police agents to the whole national territory in order to continue surveillance of people or the transport of goods[14] and protective measures of criminal assets[15]. Thus, no special investigation techniques comparable to intelligence-gathering techniques can be implemented.

10. See 1) and 2) of Article 706-73-1 of the French Criminal Procedure Code.
11. See 6) of Article 706-73-1 of the French Criminal Procedure Code.
12. The provisions of Article 706-88 of the French criminal procedure code are therefore not applicable to these offences, which in particular allow the duration of police custody to be extended to 96 hours and the intervention of the lawyer to be postponed.
13. See decision no. 2015-508 QPC of 11 December 2015, Mr Amir F. [*Exceptional extension of police custody for acts of money laundering, receiving stolen goods and criminal conspiracy in connection with acts of fraud in organised gang*], recital 13.
14. See Articles 706-80 *et seq.* of the French Criminal Procedure Code..
15. See Article 706-103 of the French criminal procedure code.

In parallel with these provisions of the French criminal procedure code, the last paragraph of Article 414 of the French Customs Code punishes the offences of smuggling and import or export without declaration of prohibited goods in an organised gang. The procedural regime applicable to these offences is that provided for by the customs code which also includes special investigation procedures. These offences have also recently been added to those mentioned in Article 706-73 of the French criminal procedure code by Law no. 2023-610 of 18 July 2023 aimed at giving customs the means to deal with new threats[16].

1.1.3. | Offences falling under specialized jurisdictions

In addition to those already mentioned, other offences may give rise to the application of the exceptional procedural regime provided for organized crime and delinquency as long as their complexity justifies that they fall within the jurisdiction of certain specialized courts.

Thus, Article 706-1-1 of the French criminal procedure code provides that certain offences fall within the jurisdiction of the national financial prosecutor's office[17] may give rise to the application of all rules derogating from common law with the exception of those relating to police custody and searches outside legal hours[18]. This regime is particularly applicable to the offence of corruption, influence peddling, or embezzlement (without requiring the circumstance of an organized gang), as well as to tax evasion and illegal taking of interests when they are committed in organized gangs.

Certain offences falling within the jurisdiction of public health centres, notably aggravated drug trafficking, may also be subject to an exceptional investigation regime, although more restrictive than that previously mentioned[19].

16. See Article 29 of the Law adding a 21) to Article 706-73 of the French criminal procedure code.
17. See Articles 705 *et seq.* of the French Criminal Procedure Code..
18. See Articles 706-89 to 706-94 of the French criminal procedure code.
19. See Article 706-2-2 of the French criminal procedure code.

In the sense of criminal law and criminal procedure, the notion of delinquency and organized crime therefore covers a plurality of more or less serious offences falling under distinct procedural regimes.

1.2. The concept of organised crime within the meaning of the French Internal Security Code is more restrictive

1.2.1. The strict interpretation retained by the former National Commission for the Control of Security Interceptions (CNCIS) within the framework of the Law of 10 July 1991

Since the intervention of Law No. 91-646 of 10 July 1991 relating to the secrecy of correspondence sent by telecommunications[20], the prevention of delinquency and organized crime was among the purposes enabling the implementation of security interceptions for intelligence purposes.

Brought to specify the scope of application of this purpose, the CNCIS had considered, before the introduction of a derogatory procedural regime applicable to organised crime in the French criminal procedure code, that were likely to be presented for the purpose of preventing organised crime, requests concerning not only offences committed by organised gangs, but also those involving a certain degree of organisation, that is to say a certain distribution of roles[21].

After the intervention of the aforementioned Law of 9 March 2004, the Commission adopted a definition of the purpose covering "totally the field covered by Article 706-73 of the French criminal procedure code"

20. See Article 3 of the law, subsequently codified in Article 241-2 of the French Internal Security Code.

21. See the 2002 CNCIS activity report, pp. 68 to 72.

thereby excluding "most of the financial offences committed by an organised gang [falling] largely under article 706-74 of the French criminal procedure code." It nevertheless allowed the inclusion in the scope of the purpose of offences which, although not covered by Article 706-73, were likely to cause harm to life or, in a serious manner, to public health. She thus considered with regard to these offences that "the extent of the alleged trafficking, the methods of committing the proposed offences (in particular their international aspect), the risks of harm to the health of the victims" presented effects "comparable" to the interests protected by the incriminations of Article 706-73, justifying favourable opinions on a case-by-case basis "to the extent that the facts were of the exceptional nature established by law to authorise a security interception"[22].

1.2.2. An interpretation reinforced by the intervention of the law of 24 July 2015 and informed by the decision of the Constitutional Council of 23 July 2015

During the parliamentary debates relating to the law of 24 July 2015 relating to intelligence, the Government opposed an amendment intended to limit the scope of application of the purpose compared to what was previously provided for in the Article L. 241-2 of the French Internal Security Code by restricting it to crimes and offences punishable by at least five years of imprisonment. It argued that the terms "organised crime" referred, as the opinions of the CNCIS had shown, to the offences referred to in Article 706-73 of the French criminal procedure code, all punishable by a custodial sentence. of freedom exceeding five years[23].

In its decision of 23 July 2015[24], the Constitutional Council, while citing the overly broad and insufficiently defined nature of the purposes listed in the new Article L. 8113 of the French Internal Security Code, considered that the law-maker had precisely limited the purpose mentioned in 6° of this article and retained criteria in line with the objective

22. See the 2014- 2015 CNCIS activity report, pp. 130- 131.

23. See the report of the debates in public session at the National Assembly (1st reading), second session of 13 April 2015, on amendment no. 108 presented by Mr Morin and others on 9 April 2015 (rejected).

24. See decision no. 2015-713 DC of 23 July 2015 recital 10.

pursued by referring to "the criminal offences listed in Article 706-73 of the French criminal procedure code and the offences punishable by Article 414 of the French customs code committed as an organised gang."

This reference to the provisions of the last paragraph of Article 414 of the French Customs Code does not appear in the parliamentary debates but appears, however, in the observations presented by the Government before the Constitutional Council[25] in consistency with the procedural regime applicable to the offences concerned.

1.2.3. The impact of subsequent amendments to criminal law and criminal procedure

The CNCTR has endeavoured to construct a doctrine making it possible to delimit the outline of this purpose by interpreting the scope of the various subsequent interventions by the legislator leading to the creation of new offences or the establishment of new procedural rules in the field of organised crime, in the light of the decision of the Constitutional Council of 23 July 2015.

In this regard, it considered that this decision had neither the purpose nor the effect of "crystallising" the list of offences whose prevention is likely to justify the implementation of an intelligence-gathering technique by limiting it to offences mentioned in Article 706-73 of the French criminal procedure code in the version in force on the date of the decision of the Constitutional Council.

It therefore selects a double material criterion relating, on the one hand, to the reality of an action "in an organized gang", in accordance with the approach of the Constitutional Council and the jurisprudence of the Court of Cassation, and on the other hand , to the degree of seriousness or dangerousness of the threat that must be prevented, justifying the use of monitoring techniques prior to possible legal proceedings. It also takes

25. See the Government's observations before the Constitutional Council according to which: "the notion of organised crime refers to the provisions in Article 706-73 of the CPP which lists crimes and offences allowing the use of special investigative techniques, as well as offences punishable by Article 414 of the French Customs Code when they are committed in an organised gang."

into account a procedural element by investigating whether special investigative techniques, comparable to the techniques covered by the French Internal Security Code, are likely to be implemented for the investigation, detection and prosecution of these offences.

Thus, with regard to offences which are not covered by the provisions to which the Constitutional Council expressly referred in its decision of 23 July 2015, the CNCTR considers that the use of intelligence-gathering techniques for the prevention of organised crime within the meaning of the French Internal Security Code can only concern offences which, like those mentioned in Articles 706-73 of the French criminal procedure code and 414 of the French Customs Code, fall under "serious organised crime".

The Commission therefore considered that the offences mentioned in Article 706-73-1 of the French criminal procedure code[26], which was introduced into positive law following the intervention of the decision of the Constitutional Council of 23 July 2015[27], entered into also within the scope of this purpose.

Indeed, the offences committed with the circumstance of the organised gang present a significant degree of seriousness and the procedural regime derogating from common law which applies to them is almost identical to that provided for the offences mentioned in Article 706-73 of the French criminal procedure code. All of the special investigative techniques, particularly harmful to privacy, applicable to the offences mentioned in Article 706-73 also apply to them.

Conversely, the Commission considers that the prevention of offences which, although committed under the circumstances of an organised gang within the meaning of the French Criminal Code, fall under the regime provided for by Article 706-74 of the French criminal procedure code (for example with regard to trafficking of false documents by organised gangs) does not allow the use of intelligence-gathering

26. Such as the offence of organized gang fraud or the offences of concealing activities or employees, using the services of a person carrying out concealed work, bargaining for labour, illicit lending of labour work or employment of a foreigner without a work permit, committed in an organized gang.

27. See point 1.1.2 above.

techniques. On the one hand, Article 706-74 of the French criminal procedure code had already been introduced into positive law on the date on which the decision of the Constitutional Council of 23 July 2015 took place and it included provisions similar to those currently in force with regard to the procedural regime derogating from the applicable common law. On the other hand, the regime applicable to the offences mentioned in Article 706-74 is largely comparable to that provided for ordinary law offences, allowing the use of only a limited number of special investigation techniques.

Likewise, the Commission did not consider it possible to extend the scope of "purpose 6" to offences likely to fall under specialised jurisdictions such as the national financial prosecutor's office (for example, crimes of corruption, influence peddling, or illegal taking of interests, or even insider trading) or public health centres (trafficking in doping products). Even though the procedural regime applicable to these offences allows the implementation of particularly intrusive investigative techniques, it noted that the provisions of Article 706-1-1 of the French criminal procedure code, which mention various offences in matters economic and financial, were already in force on the date on which the decision of the Constitutional Council was taken and that they had therefore voluntarily been excluded from the scope of "purpose 6".

With regard to persons likely to be targeted by intelligence-gathering techniques based on the purpose of the prevention of organised crime, consistent with the requirement of "presumption of direct and personal involvement"[28] in light of which the requests addressed to it are examined, the CNCTR considers that only persons likely to be involved as perpetrators or accomplices of offences falling within the scope of the purpose may be subject to such techniques. It was therefore able to issue negative opinions on requests relating to an alleged victim of pimping or even with regard to a user of narcotic products due to a lack of evidence allowing the possible involvement of this user in trafficking.

28. See Study 2 of this report "Should the people in close contact with monitored individuals be under surveillance?" here below.

2. A purpose which presents a particular challenge for respecting the scope of intervention of the administrative police in relation to legal procedures

The commission also ensures that the action of the intelligence services in the field of prevention of delinquency and organized crime does not encroach on the prerogatives of the competent judicial authority for the investigation and prosecution of offences.

Indeed, in its aforementioned decision of 23 July 2015, if the Constitutional Council considered that the law-maker had precisely limited the outline of the purpose tending to the prevention of organised crime, it first recalled that the collection intelligence using the techniques defined in Title V of Book VIII of the French Internal Security Code, which falls under the administrative police, could have "no other aim than to preserve public order and prevent offences" and, consequently, that it could not be implemented "to record violations of criminal law, gather evidence or seek out the perpetrators"[29].

Through its opinions, the CNCTR has therefore endeavoured to identify a doctrine intended to guarantee respect for the respective fields of intervention of the administrative police and the judicial authority (2.1).

However, the examination of the requests submitted to the Commission on the basis of "purpose 6" highlighted the need, to concretely ensure this respect, for a close dialogue between the intelligence community and the judicial authority. The evolution of serious organised crime disputes makes it crucial today to implement a real, flexible and efficient connection between the administrative and judicial fields (2.2).

29. See decision mentioned above, recital 9.

2.1. The necessary delimitation of the field of intervention of administrative surveillance in relation to judicial procedures

2.1.1. The principles of separation of powers and respect for the field of intervention of the judicial authority

The legality control carried out by the Commission as part of the examination of the requests for intelligence-gathering submitted to it necessarily includes a control of compliance with the principle of separation of powers as explained by the Constitutional Council in its decision of 23 July 2015 cited above, from which follows respect for the respective fields of intervention of the administrative police and the judicial authority in this matter. The collection of information using the techniques mentioned in the French Internal Security Code can therefore only have the aim of preserving public order and preventing offences. The judicial police, for their part, are solely competent to report violations of criminal law, gather evidence and seek out the perpetrators.

The examination by the Commission of requests for intelligence-gathering techniques presented on the basis of "purpose 6" is therefore particularly attentive both with regard to the incriminating texts referred to by the service in support of its request[30] and with regard to the facts which the service intends to notify the Commission and the stage of their characterisation.

The CNCTR is particularly keen to ensure that there is no criminal offence already noted which would justify immediate referral to the judicial authority and would therefore call for a negative opinion on the implementation of administrative monitoring techniques.

30. The same request could thus receive, successively, a negative opinion for lack of mention of a legal basis falling within the scope of the purpose, then favourable since the last paragraph of Article 414 of the French Customs Code was mentioned. In this regard, the CNCTR admitted that an intelligence service other than the National Directorate of the Intelligence and Customs Investigations (DNRED) requests intelligence-gathering techniques in order to prevent the threat linked to trafficking which would fall under the provisions of Article 414. of the French Customs Code (without being mentioned by the provisions of Articles 706-73 and 706-73-1 of the French criminal procedure code), since the elements allow us to suspect that the acts were committed by an organised gang.

It thus ensures that "purpose 6" is not invoked in any way "diverted", to allow the use of an intelligence-gathering technique provided for by the French Internal Security Code in a situation where the possibility of using the similar special investigation technique provided for by the French criminal procedure code would appear more uncertain to the service.

The commission is also particularly vigilant in cases where there is "back and forth" between the administrative and judicial frameworks, for example when a judicial investigation is opened on the basis of administrative information for the purposes of implementing special techniques. of investigation provided for by the French criminal procedure code, then closed for the purposes of opening a new administrative phase on the basis of the French Internal Security Code intended to ultimately allow the opening of a judicial investigation. These configurations indeed carry a major procedural risk both with regard to the principle of legality and the principle of fairness in the collection of evidence.

2.1.2. A border that is sometimes difficult to draw which has led the CNCTR to adapt its opinions

In practice, the precise moment when the period of prevention has ended because the offence has begun to be executed can be difficult to characterize.

The commission, however, takes into account the possible "divisibility" of surveillance. Thus, when certain conditions are met, it can issue favourable opinions even in cases where the judicial authority is seized or could be seized. These favourable opinions are, however, accompanied by a restriction "with the exception of facts which are before the judicial authority" which has the effect of prohibiting the service from searching for elements linked to offences already the subject of an investigation. legal proceedings or which the judicial authority should take up imminently.

In practice, two hypotheses can be distinguished in this respect:

- the request mentions offences of which the judicial authority has already been notified, but whose nature or the context in which they were committed make it particularly likely that they will be repeated by the target that the service intends to prevent;

- the target is the subject of legal proceedings for certain facts, but the service mentions in its request distinct facts covering a different criminal classification, in which this target would also be likely to be involved.

Furthermore, while there are elements that allow us to consider that the characterisation of an offence is emerging, the service may be able to indicate that it has already communicated the information in its possession to the judicial authority, where appropriate within the framework of the provisions of Article 40 of the French criminal procedure code, to allow the opening of a judicial investigation, but which the latter has not, as it stands, taken up. In this last hypothesis, the commission may be required to issue a favourable opinion "to confirm the personal involvement of the target in connection with the reason requested" or for a final monitoring before referral to the judicial authority.

This concern for pragmatism should not hide the need for a more structured dialogue between the intelligence services and the judicial authority, both to ensure the effectiveness of respect for the principle of separation of powers and to make it possible to hinder very serious organized crime in the most efficient way possible.

2.2. The need to improve exchanges between the intelligence services, the commission and the judicial authority in order to avoid difficulties harmful to their respective missions

2.2.1. A shared need for concertation

The development of better consultation between, on the one hand, the commission and the intelligence services, and on the other hand, the intelligence services and the judicial authority, meets a dual objective of protecting the operational capacities of the services and securing criminal procedures.

By strengthening the control and fluidity of the relationship between intelligence services and judicial authorities, it is thus a question of encouraging the action of intelligence services where it is justified, with the ultimate objective of judicial obstruction. It is also a question, in determining the most appropriate moment to make the switch from the administrative framework to the judicial framework, of not "adjudicating" the information obtained either too far upstream, at a stage where the judicial authority does not have sufficient elements to seize or to usefully continue the investigations, nor too downstream, at a stage where the legality of the implementation of intelligence-gathering techniques would be in question.

Despite different practices depending on the services and the difficulty in drawing a precise boundary between the scope of administrative surveillance and that of judicial procedures, the commission strives to establish a coherent doctrine in the interest of predictability of its opinions and respect for the principle of separation of powers. It can thus invite the intelligence services to contact the competent judicial authority so that the latter considers taking up the facts for which the granting of an

intelligence-gathering technique is requested, since in view of the elements presented to support this request, the conditions for such a referral appear to be met. It may be required to give favourable opinions "to adjudicate", accompanied by a short deadline, when the elements collected by the service, without yet formally characterising an offence, make it possible to envisage a referral to the judicial authority in the short term.

The commission's ex-post control activity also highlighted, through the exchanges taking place in this context with the intelligence services, that the services were themselves in need of better coordination with the judicial authority. Indeed, taking into account the principle of primacy of the judicial over the administrative, the implementation of a special investigative technique against a person within the framework of a legal procedure can, in certain hypotheses, lead to the automatic interruption of an Intelligence-gathering technique implemented by an intelligence service in application of the provisions of the French Internal Security Code without the latter being informed, nor having knowledge of the exact scope of the referral of the judicial authority.

It is in order to respond to these difficulties that the law-maker also established, by law no. 2021-998 of 30 July 2021 relating to the prevention of acts of terrorism and intelligence, known as PATR, a legal framework allowing exchanges between the intelligence services and the judicial authority, without disregarding the provisions of Article 11 of the French criminal procedure code[31]. It thus provided, in article 706-105-1 of the French criminal procedure code, that, in certain areas, such as cybercrime and very complex organised crime falling under the national jurisdiction responsible for the fight against organised crime (JUNALCO)[32], the Paris prosecutor can communicate elements contained in legal proceedings relating to certain offences to the first-line intelligence services and to certain services of the second line[33].

31. Article 11 of the French criminal procedure code provides that: "Except where the law provides otherwise and without prejudice to the rights of the defence, the procedure during the investigation and investigation is secret. Any person who participates in this procedure is bound by professional confidentiality under the conditions and under the penalties provided for in Article 434-7-2 of the French Criminal Code.

32. See Article 706-75 of the French criminal procedure code.

33. Similar provisions pre-existed regarding the prevention of terrorism, see in this regard Article 706-25-2 of the French criminal procedure code.

2.2.2. Prospects for encouraging these exchanges

As part of its ex-ante control as well as its ex-post control, the CNCTR must ensure compliance with the scope of intervention of the judicial authority when judicial and administrative proceedings coexist against the same individual. To this end, it appears essential that the CNCTR is systematically made the recipient of all the necessary elements enabling it to render its opinions in an informed manner.

However, this information cannot be obtained directly from the judicial authority. Although the commission regularly meets public prosecutors from certain judicial courts as part of its travels in the territory in order to discuss the specificities of local delinquency and crime, it cannot send a request for information on specific cases. The rules for preserving national defence secrecy are in fact opposed to this.

It is therefore necessary for the intelligence services to provide the information essential to monitoring compliance with the competence of the judicial authority in the motivation of their requests for intelligence-gathering techniques to the Commission.

This concern must also make it possible, via reinforced communication with the judicial authority, to immediately establish whether or not a threat distinct from the facts already before it has been identified.

Summary table of offences falling within the scope of "purpose 6"

OFFENCES LIKELY TO FALL WITHIN THE SCOPE OF THE PURPOSE OF ARTICLE 706-73 (6) OF THE FRENCH CRIMINAL PROCEDURE CODE			
CLASSIFIED AS ORGANISED CRIME BY	**OFFENCES**	**REQUIREMENT ORGANISED GANG**	**FRENCH INCRIMINATING TEXTS**
706-73, 1°	Organized gang **murder**	YES	**Criminal Code, Art. 221-1 and 221-4 8°**
706-73, 2°	**Torture** or **barbaric acts** by organized gang	YES	**Criminal Code, Art. 222-1 and 222-4**
706-73, 2°bis	**Rape in conjunction** with one or more other rapes committed against other victims	NO	**Criminal Code, Art. 222-23**
706-73, 3°	**Drug trafficking**	NO	**Criminal Code, Art. 222-34 to 222-40**
706-73, 4°	**Kidnapping** or **sequestration**	YES	**Criminal Code, Art. 224-1 and 224-5-2**
706-73, 5°	**Trafficking of human beings aggravated** by one of the aggravating circumstances provided for by Articles 225-4-2 to 225-4-4 of the French Criminal Code, including BO	NO	**Criminal Code, Art. 225-4-1 to 225-4-4.**
706-73, 6°	**Procuring aggravated** by one of the aggravating circumstances provided for by Articles 225-7 to 225-12 including the Commission in meeting, with regard to several victims, with regard to a minor and the BO	NO	**Criminal Code, Art. 225-5 and 225-6** **Criminal Code, Art. 225-7 to 225-12**
706-73, 7°	Organized gang **theft**	YES	**Criminal Code, Art. 311-9**
706-73, 8°	Criminal **extortion** provided for by Articles 312-6 or 312-7 of the French Criminal Code: in an organised gang, **or** with acts of torture and barbarity, **or** with violence resulting in death	NO (see other circumstances)	**Criminal Code, Art. 312-1 § 1,** **Criminal Code, Art. 312-6 and 312-7**
706-73, 9°	**Destruction, damage or deterioration of the property of others by explosive substance, fire or dangerous means for people** in organized gangs	YES	**Criminal Code, Art. 322-6 and 322-8**
706-73, 10°	**Counterfeiting (manufacturing):** counterfeiting, falsification or irregular manufacturing of coins or bank notes	NO	**Criminal Code, Art. 442-1**
706-73, 10°	**Counterfeiting (putting into circulation):** transport, putting into circulation or holding with a view to putting into circulation counterfeit, falsified or irregularly manufactured coins or bank notes	YES	**Criminal Code, Art. 442-2**

OFFENCES LIKELY TO FALL WITHIN THE SCOPE OF THE PURPOSE OF ARTICLE 706-73 (6) OF THE FRENCH CRIMINAL PROCEDURE CODE			
CLASSIFIED AS ORGANISED CRIME BY	**OFFENCES**	**REQUIREMENT ORGANISED GANG**	**FRENCH INCRIMINATING TEXTS**
706-73, 12°	**Arms and ammunition (trafficking):** illicit acquisition, possession, transfer, illicit carrying or transport, outside the home, of war materials, weapons, elements of weapons or ammunition of categories A or B. Possession of an arms depot or category A and B ammunition. Illicit importation of weapons of war, or weapons or ammunition of categories A, B, C and certain weapons of category D	**NO**	**Criminal Code, Art. 222-52** **Criminal Code, Art. 222-53** **Criminal Code, Art. 222-54** **National Defence Code, Art. L. 2339-10**
706-73, 12°	**Arms and munitions (war materiel):** illicit manufacture or trade of war material	**-**	**National Defence Code, Art. L. 2339-2**
706-73, 12°	**Weapons and ammunition (manufacture):** constitution or reconstitution of a weapon, or modification of a weapon having the effect of changing its category	**NO**	**Criminal Code, Art. 222-59**
706-73, 12°	**Weapons and munitions (explosive product):** possession or transport of incendiary or explosive substances or products, or elements included in their composition, with a view to the preparation, degradation or deterioration of property or attacks on people	**NO**	**Criminal Code, Art. 322-1-1**
706-73, 12°	**Weapons and ammunition (explosive product):** illicit manufacture of explosive or incendiary devices, explosive products, or elements or substances intended to be used in the composition of an explosive product	**NO**	**National Defence Code, Art. L. 2353-4**
706-73, 13°	**Assistance with the entry, movement and illegal stay of a foreigner** in France in an organised gang	**YES**	**Code of entry and stay of foreigners and the right to asylum, Art. L. 823-1 and L. 823-2**
706-73, 14°	**Money laundering** or **concealment** of proceeds, income or things resulting from an offence mentioned in 1° to 13° of Article 706-73 (i.e., the offences reported above).	**NO**	**Criminal Code, Art. 324-1 and 324-2** **Criminal Code, Art. 321-1 and 321-2**
706-73, 15°	**Criminal conspiracy** whose object is the preparation of one of the offences mentioned in 1° to 14° of Article 706-73 (i.e., the offences mentioned above).	**NO**	**Criminal Code, Art. 450-1**
706-73, 17°	**Hijacking of aircraft, ship or any other means of transport** in an organized band	**YES**	**Criminal Code, Art. 224-6 and 224-6-1**

OFFENCES LIKELY TO FALL WITHIN THE SCOPE OF THE PURPOSE OF ARTICLE 706-73 (6) OF THE FRENCH CRIMINAL PROCEDURE CODE			
CLASSIFIED AS ORGANISED CRIME BY	OFFENCES	REQUIREMENT ORGANISED GANG	FRENCH INCRIMINATING TEXTS
706-73, 16°	**Failure to provide proof of resources** corresponding to lifestyle in relation to one of the offences mentioned in 1° to 15° and 17° of Article 706-73 (*i.e., the offences reported above*)	**NO**	**Criminal Code, Art. 321-6 and 321-6-1**
706-73, 19°	**Environment:** exploitation of a mine or disposal of a transferable substance, without exploitation title or authorisation, with damage to the environment, in an organised gang and related to one of the offences mentioned in 1° to 17° of Article 706-73	**YES**	**Mining Code, Art. L. 512-2**
706-73, 20°	**Abuse of weakness** in an organized gang	**YES**	**Criminal Code, Art. 223-15-2**
706-73, 21°	**Customs offences:** smuggling, import or export without declaration of goods dangerous to public health, morality or security, the list of which is established by order of the minister responsible for customs, or committed in an organized gang	**NO**	**Customs Code, Art. 414, al.3**

OFFENCES LIKELY TO FALL WITHIN THE SCOPE OF THE PURPOSE OF ARTICLE 706-73 (1) OF THE FRENCH CRIMINAL PROCEDURE CODE			
CLASSIFIED AS ORGANISED CRIME BY	**OFFENCES**	**REQUIREMENT ORGANISED GANG**	**FRENCH INCRIMINATING TEXTS**
706-73-1, 1°	Organized gang **fraud**	YES	**Criminal Code, Art. 313-1 and 313-2**
706-73-1, 1°	**Attack on an automated data processing system** in an organised gang	YES	**Criminal Code, Art. 323-1 and 323-3-1** **Criminal Code, Art. 323-4-1**
706-73-1, 1°	Organized gang **escape**	YES	**Criminal Code, Art. 434-27 and 434-29 1°** **Criminal Code, Art. 434-30 § 2,**
706-73-1, 2°	**Hidden work** in an organized gang	YES	**Labour Code, art. L. 8221-1, 1° and 3°**
706-73-1, 3°	**Concealment** of proceeds, income or things resulting from an offence mentioned in 1° and 2° of Article 706-73-1 (*i.e., the offences reported above*).	NO	**Criminal Code, Art. 321-1 and 321-2**
706-73-1, 3°	**Laundering** of proceeds, income or things resulting from an offence mentioned in 1° and 2° of Article 706-73-1 (*i.e., the offences reported above*).	NO	**Criminal Code, Art. 324-1**
706-73-1, 3° *bis*	Organised gang **laundering** of any offence other than those referred to in 14° of Article 706-73 (*see table*)	YES (or habitually or facilitated by professional activity)	**Criminal Code, Art. 324-2**
706-73-1, 4°	**Criminal conspiracy** whose object is the preparation of one of the offences mentioned in 1° to 3° of Article 706-73-1 *(i.e., the offences mentioned above)*.	NO	**Criminal Code, Art. 450-1**
706-73-1, 5°	**Failure to provide proof** of resources corresponding to lifestyle in relation to one of the offences mentioned in 1° to 4° of Article 706-73-1 (*i.e., the offences reported above*)	NO	**Criminal Code, Art. 321-6 and 321-6-1**
706-73-1, 6°	**Trafficking in cultural property** stolen from a scene of terrorist operations	NO	**Criminal Code, Art. 322-3-2**
706-73-1, 7°	**Attacks on natural heritage** by organised gangs (non-domestic animal species, non-cultivated plant species, natural habitats, sites of geological interest, etc.)	YES	**Environmental Code, Art. L. 415-3 and L. 415-6**

OFFENCES LIKELY TO FALL WITHIN THE SCOPE OF THE PURPOSE OF ARTICLE 706-73 (1) OF THE FRENCH CRIMINAL PROCEDURE CODE			
CLASSIFIED AS ORGANISED CRIME BY	OFFENCES	REQUIREMENT ORGANISED GANG	FRENCH INCRIMINATING TEXTS
706-73, 8°	Organized gang **trafficking of plant protection products**	YES	**Rural and maritime fishing code, Art. L. 253-15, L. 253-16, L. 253-17-1, 3° and L. 254-12, III**
706-73, 9°	**Crimes relating to waste** by organized gangs	YES	**Environmental Code, Art. L. 541-46, I and VII**
706-73, 10°	**Gambling and gambling:** participation in running a gambling house committed by an organized gang	YES	**Internal Security Code, Art. L. 324-1, para. 1**
706-73, 10°	**Gambling and gambling:** importation, manufacture, possession, provision to third parties, installation and operation of gambling machines or games of chance committed by an organized gang	YES	**Internal Security Code, Art. L. 324-4, para. 1**
706-73, 13°	**Social fraud:** provision of instruments to facilitate social fraud in organized gangs	YES	**Social Security Code, Art. L. 114-13**

Study 2. Should the people in close contact with monitored individuals be under surveillance?

In everyday language, the entourage corresponds to "all of those who ordinarily surround someone, who live in their familiarity"[1].

In the French Internal Security Code, where the concept is mentioned in Articles L. 851-2 and L. 852-1[2], its meaning is more restricted. Should the law-maker not define they have defined the outline by establishing its regime. Thus, the entourage, within the meaning of the French Internal Security Code, corresponds to all those with regard to whom certain intelligence-gathering techniques can be implemented because they "are likely to provide information for the purpose", due to their closeness to a target in direct and personal connection with one of the purposes mentioned in Article L. 811-3 of the French Internal Security Code[3].

The possibility of monitoring members of a target's entourage was introduced into positive law by Law No. 2015-912 of 24 July 2015 relating to intelligence.

Although it does not call into question the principle of the individualised nature of intelligence-gathering techniques (1), it nevertheless constitutes a derogation from this principle according to which a person can only be the subject of technical surveillance if he/she appears personally linked with a threat to ward off or an interest to protect (2).

1. Dictionary of the French Academy.

2. Title I of Article L. 851-2 of the French Internal Security Code, relating to access to connection data in real time, provides in particular that "(...) When there are serious reasons to believe that one or more people belonging to the entourage of the person concerned by the authorisation are likely to provide information for the purpose which motivates the authorisation, this can also be granted individually for each of these people. " Title I of Article L. 852-1 of the French Internal Security Code, relating to security interceptions, provides in almost identical terms that: "When there are serious reasons to believe that one or more people belonging to the entourage of a person concerned by the authorization are likely to provide information for the purpose which motivates the authorization, this may also be granted for these people.

3. Article L. 811-3 lists seven purposes making it possible to justify the use of intelligence-gathering techniques provided for by the French Internal Security Code: 1) National independence, territorial integrity and national defence; 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; 3) The major economic, industrial and scientific interests of France; 4) The prevention of terrorism; 5) The prevention of: a) Damage to the republican form of the institutions; b) Actions aimed at maintaining or rebuilding dissolved groups pursuant to Article L. 212-1; c) Collective violence likely to seriously harm public peace; 6) Prevention of organised crime; 7) Prevention of the proliferation of weapons of mass destruction.

1. An exception to the principle according to which intelligence-gathering techniques only make it possible to monitor a person directly linked to a threat

The legal framework prior to the law of 24 July 2015[4] did not include an express legal basis for the implementation of technical surveillance with regard to a person who is part of a target's entourage (1.1). The introduction of such a possibility by the law of 24 July 2015 did not call into question the requirement for individualisation of technical surveillance, the principle remaining the prohibition of monitoring of a target's relatives as long as they are not themselves subject to authorisation (1.2).

1.1. The requirement for direct and personal involvement of people likely to be the subject of intelligence-gathering techniques before the law of 24 July 2015

1.1.1. The law of 10 July 1991 was silent as to the possibility of implementing intelligence-gathering techniques against people who, without themselves representing a threat, were likely to hold interesting information due to the close relations they have with a target.

The former Article L. 241-2 of the French Internal Security Code limited itself to providing that "could be authorised, exceptionally, in the conditions

4. See Law No. 91946 of 10 July 1991 relating to the secrecy of correspondence sent by telecommunications.

provided for in Article L. 242-1, interceptions of correspondence sent by electronic communications intended to seek information of interest to national security, the safeguarding of essential elements of France's scientific and economic potential, or the prevention of terrorism, organized crime and delinquency and the reconstitution or maintenance of dissolved groups pursuant to Article L. 212-1."

In the absence of a legal basis and despite the absence of an explicit prohibition in the law, the national commission for the control of security interceptions (CNCIS) was opposed to an interception authorization allowing the listening of "surroundings of a target [...] simply because of this quality". Each request for security interception was thus examined in the light of a requirement of "presumption of direct and personal involvement", the CNCIS verifying that the person involved was "indeed the potential author of an offence in preparation or of the act involving various national interests"[5].

1.1.2. When Law of 24 July 2015 pertaining to intelligence was introduced, it however appeared that the impossibility to place under surveillance persons in close contact with monitored individuals significantly limited the ability of intelligence services to prevent some threats.

The evolution of the threat, particularly terrorist, has first of all highlighted the major interest in information likely to be held by those close to people identified as carrying a threat. They communicate by different means with those around them who, without themselves being involved in any violent project, potentially hold information of interest relating to their activities, their location or contacts. Members of the entourage sometimes even constitute the only possible channel for collecting

5. See 23rd CNCIS activity report, 2014-2015 period, p. 21: "It is up to the Commission to verify that the person concerned is indeed the potential author of the proposed offence or of the act involving various national interests.*(...)*. The law has never provided that we can listen to "those around us" (if they are not accomplices) simply because of this quality; nor did she authorize the interception of the victims' communications."

intelligence, particularly when the main target cannot be reached by intelligence-gathering techniques[6] (for example because it is not located or because it is located abroad).

It also appeared that if the requirement of a presumption of direct and personal involvement was well suited to the search for information useful for the prevention of threats likely to receive a criminal classification, it was intellectually less appropriate when are in because of the challenges of preventing attacks on the fundamental interests of the Nation, further removed from the criminal field.

Indeed, in these areas, for example in matters of protection of the economic interests of the Nation, the purpose of surveillance is to seek relevant information that a person is likely to hold simply because of their quality or position. The latter is then not suspected of acting as a potential perpetrator of an offence in preparation, but only identified as holding or likely to hold relevant information[7].

The evolution of the threat and the need, to prevent it effectively, to be more interested in the relevant information held by certain people than in their personal involvement led the law-maker in 2015 to allow an intelligence-gathering technique to be implemented against people who are part of the entourage of the main targets. However, the principle remains that of individualized surveillance which prohibits a technique authorized against a person from leading to the surveillance of people in their entourage in the absence of authorization to this effect.

6. See the opinion of the National Commission for Information Technology and Liberties (CNIL) of 4 March 2015 on the intelligence bill, the impact study of 18 March 2015 on the intelligence bill, and report No. 2697 made on behalf of the Law Commission on the draft law relating to intelligence by Mr Jean-Jacques Urvoas, registered at the presidency of the National Assembly on 2 April 2015.

7. Thus, surveillance aimed at combating activities relating to crime or organized delinquency, or even at preventing violent behaviour, naturally concerns individuals who are suspected of culpable involvement in acts, in preparation , criminally qualifying. "Direct and personal involvement" then means elements which allow us to suspect that the individual is indeed likely to participate in one or other of the elements constituting an offence or a crime in preparation. This requirement of "guilty" involvement is, however, not relevant when the aim pursued is the search for information concerning areas such as foreign policy or the major economic, industrial or scientific interests of France.

1.2. A principle of individualisation of surveillance which has remained since 2015 and bans "collateral" surveillance

The law of 24 July 2015 maintained the principle of the individual nature of surveillance. Article L. 8212 of the French Internal Security Code resulting from this law provides that, when an intelligence service submits a request for intelligence-gathering techniques, it must specify in particular: "3° The purpose(s) pursued; 4° The reason(s) for the measures; [...] 6° The person(s), place(s) or vehicles concerned, [...] persons whose identity is not known [may] be designated by their identifiers or their status and the places or vehicles [may] be designated by reference to the persons who are the subject of the request."

If the law now provides that people who are part of targets' entourage can be subject to technical surveillance on their behalf, it is only under certain precisely determined conditions (see below). Apart from these situations and in the absence of authorisation granted specifically "in respect of the entourage", the CNCTR ensures that the surveillance of a target does not lead to that of his/her entourage (1.2.1). Its control is reinforced when the entourage of a target who is the subject of a request for an intelligence-gathering technique has a protected profession (1.2.2).

1.2.1. The control of the "collateral" monitoring of persons in close contact with monitored individuals

The CNCTR ensures that the authorised techniques do not infringe too significantly on the rights of third parties present in the entourage of a target.

As part of its ex-ante control of proportionality, it systematically verifies that the nature and extent of the attack on the privacy of people in contact with or near the main target, which is likely to result from the implementation of a technique against it, particularly in the hypothesis of capturing sound or images, are proportionate to the reality and seriousness of the threat represented by this target.

As part of its ex-post control, the commission verifies that the information finally retained by the service was indeed collected while the main target was present and that it is relevant for the prevention of the threat represented by the latter. Concerning techniques whose execution is centralized, in particular security interceptions, the Inter-Ministerial Control Group (GIC), which is responsible for this centralization, itself carries out a systematic control of the communications captured and the transcriptions made. in order to verify that the line listened to is actually used by the target referred to in the request and that the information used relates to the latter and not to their interlocutor, members of their entourage or another user of the intercepted selector.

1.2.2. The control meant to prevent a monitoring "diverted" from people who exercise a mandate or a protected profession through their entourage

When a person being monitored has, in their entourage, one or more people who has a protected profession within the meaning of the French Internal Security Code[8], the CNCTR verifies that the surveillance has not for the purpose or consequence of leading to an investigation into the protected professional activity. It thus ensures that an intelligence service cannot deploy an intelligence-gathering technique against

8. Article L. 821-7 of the French Internal Security Code prevents a member of parliament, a magistrate, a lawyer or a journalist from being the subject of an intelligence-gathering technique due to the exercise of his mandate or his profession. Article L. 854-3 also provides that: "Persons who have in France a mandate or a profession mentioned in Article L. 821-7 cannot be subject to individual surveillance of their communications due to the exercise of the mandate or profession concerned". See the CNCTR 2022 activity report, p. 93 *et seq.*

a person who is part of the entourage of a person exercising a mandate or a protected profession with the aim of gaining access to information related to the protected activity.

Concerning, for example, the close collaborator of a lawyer or a member of parliament, the Commission ensures that the supervision of this collaborator is clearly "detachable" from the activity of the lawyer or the exercise of the mandate of the parliamentary[9]. As part of its ex-post control, it also carries out a systematic verification of the productions collected by the service.

The principle of individual surveillance therefore remains. If a target's entourage can now be subject to technical surveillance, the intelligence services must, to do so, obtain specific authorisation.

2. The possibility of a strictly supervised surveillance of the entourage

Surveillance of the target environment can only be considered within the framework of an authorisation regime defined by law (2.1) and a definition of the outline of the concept of environment developed by the CNCTR in order to prevent any monitoring not strictly necessary (2.2).

9. As part of its ex-ante control, the CNCTR therefore examines the request for technical surveillance in plenary session. Article L. 821-7 of the French Internal Security Code provides that "When such a request [to implement an intelligence-gathering technique] involves one of these people or their vehicles, their offices or homes, the opinion of the National Oversight Commission for Intelligence-Gathering Techniques is examined in plenary session" which corresponds to the most solemn composition of the Commission which includes all the members mentioned in Article L. 831 -1 of the French Internal Security Code as per its Article L. 831-2 and which can only validly deliberate if at least four of the nine members are present as per Article L. 832-3.

2.1. The gradual and limited implementation of technical surveillance of the entourage

Article L. 852-1 of the French Internal Security Code, created by the law of 24 July 2015 relating to intelligence, now provides that those close to a monitored person may be subject to security interception (2.1.1). This possibility has since been extended to less intrusive techniques (2.1.2).

2.1.1. The opening of the monitoring of the entourage to security interceptions

Article L. 852-1 of the French Internal Security Code provides for the possibility of implementing a security interception against a person who is part of a target's entourage: "When there are serious reasons to believe that one or more people belonging to the entourage of a person concerned by the authorization are likely to provide information for the purpose which motivates the authorization, this may also be granted for these people."

This formulation results from extensive debates during parliamentary proceedings during which fears about the emergence of generalized surveillance were expressed. During the debates in the National Assembly, a requirement was expressly added relating to the accuracy of the indications enabling to support surveillance[10]. The objective is thus to limit the number of individuals likely to be targeted as part of the entourage, whereas the initial text aimed not only at holders of information of interest, but also at people likely to play a role as an intermediary, voluntarily or not. This notion of "involuntary intermediary", which was supposed to cover

10. See amendment No. 44 of 7 April 2015, presented by Mr Coronado and others, adopted during the debates in public session at the National Assembly which led to the intermediate drafting: "When there are serious reasons to believe that one or more people belonging to the entourage of a person concerned by the authorization are likely to play an intermediary role, voluntary or not, on behalf of the latter or to provide information for the purpose for which the authorization is granted, it may also be granted for these persons.

the case of a person whose means of communication are used by the main target, even without his knowledge, was ultimately judged to be too imprecise during the debates in the Senate with the risk of an invasion of the privacy of potentially too many people. The reformulation adopted aimed to only allow the surveillance of a person close to a target "as long as they can provide information relating to the intended purpose"[11].

In its decision no. 2015-713 DC of 23 July 2015, the Constitutional Council admitted the conformity with the Constitution of this possibility of implementing security interceptions with regard to a target's entourage, considering that the law-maker had not "achieved a manifestly unbalanced conciliation between, on the one hand, the prevention of attacks on public order and that of offences and, on the other, the right to respect for private life and the secrecy of correspondence"[12]. Among the guarantees provided by the legislator, the Constitutional Council noted in particular that the execution of security interceptions was "centralized", which allowed easier control of the CNCTR, and that the number of security interceptions simultaneously implemented was limited.

2.1.2. The monitored broadening of the surveillance of the entourage to include less intrusive techniques

Driven by considerations similar to those which prevailed during the debates relating to the law of 24 July 2015, the law-maker opened real-time access to the technical connection data of the entourage by Law no. 2016-987 of 21 July 2016 extending the application of Law No. 55-385 of 3 April 1955 relating to the state of emergency and establishing measures to strengthen the fight against terrorism in the following terms: "When there are compelling reasons to believe that one or more people belonging to the entourage of the person concerned by the authorisation are likely to provide information for

11. See amendment No. COM-75 from the rapporteur of the Senate Law Committee, Mr Philippe Bas.

12. See decision no. 2015-173 DC of 23 July 2015, recitals 64 *et seq.*

the purpose which motivates the authorisation, the latter may also be granted individually for each of these people"[13].

This provision, written in terms very similar to those used for security interceptions, was declared unconstitutional by the Constitutional Council. Indeed, seized of a priority question of constitutionality relating to the provisions of Article L. 851-2 of the French Internal Security Code, the Constitutional Council censured the absence of limitation on the number of authorisations likely to be simultaneously in force. In its decision no. 2017-648 QPC of 4 August 2017, it thus considered that by allowing "a large number of people to be the subject of this intelligence-gathering technique, without their link with the threat being necessarily close" and "failing to have provided that the number of authorisations simultaneously in force must be limited", "the law-maker [had] not achieved a balanced conciliation between, on the one hand, the prevention of breaches of public order and offences and, on the other, the right to respect for private life"[14].

To comply with the requirements of the Constitutional Council, the legislator, by Law no. 20171510 of 30 October 2017 strengthening internal security and the fight against terrorism, chose to reestablish the system provided for by the law of 21 July 2016 in establishing a maximum number of authorisations that can be in force simultaneously with regard to the technique of real-time access to connection data[15]. The "compelling reasons" retained by the law of 21 July 2016, however, were once again on this occasion "serious reasons" to believe that surveillance of those close to them is likely to provide information for the purpose.

Furthermore, the authorisation to intercept a person's communications constitutes authorisation to access their internet connection data in deferred time[16], the CNCTR admits that part of this data may also be the subject of authorisations to access aimed at people who are part

13. See the provisions of Article L. 851-2 of the French Internal Security Code.

14. See decision no. 2017-648 QPC of 4 August 2017, recital 11.

15. See Article 8 of Law no. 2017-1510 of 30 October 2017 strengthening internal security and the fight against terrorism.

16. Under the provisions of Title III of Article L. 852-1 of the French Internal Security Code.

of the targets' entourage. Indeed, certain connection data which makes it possible to know the identity of people who are part of a target's entourage, or even their own contacts, are in reality collected with the aim of monitoring the main target by making it possible to map their relationships.

Finally, the Commission accepts that a person in the entourage of a target may be the subject of an authorisation to operate their international communications; this technique can be assimilated to a security interception within the framework of the measures surveillance of international electronic communications provided for in Articles L. 854-1 *et seq*. of the French Internal Security Code. Such authorisation is, moreover, subject to the same control by the CNCTR and compliance with a maximum number of authorisations simultaneously in force[17], procedural guarantees deemed sufficient by the Constitutional Council in its aforementioned decisions to allow surveillance of the entourage.

This quota of authorizations makes it possible to characterize "the close link" required by the Constitutional Council in its decision of 4 August 2017 mentioned above between people likely to be the subject of an intelligence-gathering technique and a threat, and constitutes in this regard a "powerful regulatory factor" according to the terms used by the public rapporteur of the Council of State in their conclusions relating to the so-called "French Data Network" case[18].

It is on the one hand by controlling the existence of this close link between the person likely to be the subject of an intelligence-gathering technique as part of the entourage and a threat, on the other hand, by the development of a doctrine aimed at clarifying the outline of this notion of entourage that the CNCTR strives to preserve the balance between the objective of preventing attacks on the interests of the Nation

17. See the provisions of Article L. 854-2 of the French Internal Security Code.

18. See conclusions of Mr Alexandre Lallet, master of requests of the Council of State, public rapporteur, on EC decisions, 21 April 2021, French Data Network and others, No. 393099 – La Quadrature du Net and others, No. s 394922 , 397851– Igwan Association. net, no. 397844 – Free mobile company, no. 424717 - Free company, no. 424718, noting that: "The quota of authorizations which the [Constitutional] Council considered essential to ensure respect for the Constitution, constitutes a powerful regulatory factor in this regard. *From the moment this close link is characterized, we can consider that there is a form of involvement in the sense understood by the Court [of Justice of the European Union]."*

and the right to respect for private life . In this regard, during the debates relating to the aforementioned law of 30 October 2017, the Law Committee of the National Assembly noted that:"it will be up to the Prime Minister, after consulting the CNCTR, to ensure that the person concerned by the collection request really belongs to the entourage of a person previously identified as being a threat in view of the nature of the links, their intensity, their regularity and any other element likely to justify the validity of the measure"[19].

2.2. Gradually defining the outline of the entourage concept

If the main target does not necessarily have to be the subject of monitoring techniques strictly identical to that envisaged for a person belonging to their entourage, the threat they pose shall be sufficiently identified and detailed (2.2.1). The CNCTR also clarified the scope of people likely to be effectively targeted by an intelligence-gathering technique "on behalf of the entourage" (2.2.2).

2.2.1. The existence of a main target considered as a sufficiently established threat, whether they are being monitored or not

Faced with a certain ambiguity in the provisions of the French Internal Security Code which provide for the possibility of surveillance of a target's entourage by mentioning "the entourage of a person concerned by the authorisation"[20], the CNCTR, relying on particularly on the individual

19. Report No. 164 from the Laws Committee on the bill adopted by the Senate strengthening internal security and the fight against terrorism (No. 104) by Mr Raphaël Gauvain.

20. This wording results from an amendment No. CL 187 of 31 March 2015 presented by Mr Jean-Jacques Urvoas, rapporteur of the law committee at the National Assembly, amending the initial wording which referred to the entourage of a person "covered by the authorization".

nature of surveillance and on the principle of subsidiarity, does not require that the person actually targeted be the subject of an intelligence-gathering technique identical to that requested for a member of their entourage, nor even that they be the subject of any technique.

Another interpretation of the provisions of the French Internal Security Code relating to the entourage would have been likely to result in a paradoxical situation, moreover contrary to the spirit of the law as it results from the examination of the parliamentary debates. It would in fact have led to the consideration that when a target represents such a threat that the implementation of particularly intrusive techniques such as a sound system in his/her home or the collection of his/her computer data would be authorised against him/her, those around him/her could not be the subject of a security interception authorisation, even though this monitoring technique is less intrusive, if the main target is not itself the subject of this technique. Likewise, the surveillance of relatives of a person who would pose, from abroad, a clear threat against the fundamental interests of the Nation, would not be possible since the latter, being outside of the national territory, is not likely to be targeted by an intelligence-gathering technique relating to domestic surveillance.

The reality of the threat is therefore not assessed solely in terms of the techniques actually authorized against the main target. In this regard, the CNCTR carries out a case-by-case analysis of all the elements presented by the services in their motivations in order to verify that this main target does indeed represent a threat.

The CNCTR ensures that the services provide sufficient information in this area in their requests. The main target must therefore be identified or identifiable. If his identity is unknown, the request must detail the elements making it possible to determine his personal involvement for the purpose which justifies the implementation of technical surveillance. The existence of intelligence-gathering techniques implemented with regard to the main target nevertheless remains an important criterion of assessment.

2.2.2. A person likely to hold information due to their being in close contact with a target

The technical monitoring of certain people who are part of a target's entourage does not, however, always fall under surveillance "in respect of the entourage" within the meaning of the provisions of the French Internal Security Code.

Indeed, people who are part of a target's entourage are, first of all, likely to be monitored for their personal involvement. Thus, when the service reports elements suggesting that the person is suspected of knowingly providing assistance to the main target, authorization is granted on the basis of the personal involvement of this person, who, more than a close relative, can be assimilated to an accomplice. The anchoring of a person within a movement or group which is a proven attack on the fundamental interests of the Nation may also be such that it sufficiently characterizes that he or she is in fact personally involved.

Once authorisation has been granted based on the person's personal involvement, the range of intelligence-gathering techniques that can be implemented broadens. The CNCTR does not, however, carry out an automatic reclassification of a request targeting a person solely on the basis of the entourage considering, on the one hand, that this would go beyond this request, which is not the function of the commission, on the other hand, in practice, that the surveillance of a target as part of the entourage does not in any case represent an obstacle to the service collecting and exploiting elements which would establish that the person actually represents a threat themselves.

When a person who is part of a target's entourage is not themselves involved in the identified threat, the CNCTR checks that they are sufficiently close to this main target. It thus excludes surveillance of the "indirect entourage" of a target and requires that the service

provide sufficient information to determine the nature and intensity of the links which unite the main target to the person being the subject of the request for technical surveillance "on behalf of the entourage". It also checks the current nature of the links with this main target.

Thus, requests reporting hypothetical or overly old links are at least the subject of requests for additional information intended to investigate the intensity and timeliness of these links and, where applicable, negative opinions.

Beyond that, the CNCTR above all verifies that the service sufficiently reports the existence of serious indications that the target holds information of interest relating to the main target. The possession of information of interest constitutes in fact the most important demonstration element to characterize. If it is completed, the CNCTR admits, for example, that the person likely to hold such information in relation to a target of interest is not identified by the service at the time it makes its request.

These clues may result from strong close ties between the two people or from the fact that the person identified as part of a target's entourage is likely to be the holder of media or documents belonging to the latter. The service must, in any case, designate as precisely as possible the information that the person is likely to hold, as well as their link with the main target and the purpose pursued by the surveillance.

Insights

Insight 1. Artificial intelligence (AI) and intelligence-gathering operations

Insight 2. The sensible use of commercial capabilities of cyber-intrusion: a diplomatic outlook

(Contribution from Mr Henri Verdier, the French Ambassador for Digital Affairs, and Mr Léonard Rolland, the Cybersecurity Officer, Sub-Directorate for Strategic Affairs and Cybersecurity and Disarmament for Ministry of Foreign Affairs).

Insight 1. Artificial intelligence (AI) and intelligence-gathering operations

"Like the steam engine or electricity in the past, AI is transforming our world, our society and our industry (...) / Our approach to AI will define the world in which we live." This is how the European Commission, in its communication of 25 April 2018 on artificial intelligence (AI) for Europe[1], introduced the challenges of developing a technology presented as one of the most innovative and strategic of the 21st century, to the point of making it the initiator of a 4th industrial revolution.

Five years later, 2023 turned out to be particularly rich in news on this theme, which began with the discovery by the general public of the ChatGPT[2] conversational robot deployed in open access by the Californian company OpenAI, and ended on 8 December with the announced political agreement within the European Union[3] to regulate the use of artificial intelligence by means of an *ad hoc* regulation (draft regulation **defining harmonised rules concerning artificial intelligence** or *Artificial Intelligence Act*, AI Act).

The concept of AI, born in the 1950s in cybernetics[4] circles and long relegated to the field of science fiction, has never been as present in the public debate, the succession of announcements on the advances made in matter in a number growing sectors finding echo in the proliferation of reflections and questions on the ethical and societal issues raised.

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 25 April 2018, Artificial Intelligence for Europe, COM (2018) 237 final.
2. Open access deployment at the end of November 2022 of Chat GPT (Chat Generative Pre-trained Transformer (version GPT3.5), technology allowing the generation of text autonomously by artificial intelligence.
3. Political agreement of the European Parliament and the Council on the artificial intelligence regulation, proposed by the Commission in April 2021.
4. The formalisation of the concept is generally dated from the conference organised in the summer of 1956 by John McCarthy and Marvin Minsky at Dartmouth College (New Hampshire, United States). Shortly before, Alan Turing, considered as one of the founding fathers of AI with John Von Neumann, John McCarthy and Marvin Minsky, published in 1950 an article entitled *Computing Machinery and Intelligence* questioning in an unprecedented way the limit between humans and the machine.

The present study does neither define AI, nor does it even claim to choose among the numerous existing definitions which can refer to a scientific discipline, the aim of which is to succeed in having a machine imitate the cognitive capacities of a human being[5], as well as concrete technologies that come from this academic field of research[6/7]. In a pragmatic approach, this introduction is limited to delimiting the field of reflection, which concerns the impacts and issues, in the field of intelligence, of any automated process which, from received data, generates results such as content, forecasts, recommendations or decisions. The selected systems – hereafter referred to as "artificial intelligence system" or "AIS" – include complex automated processing of data management and all algorithm techniques and student systems, with the exception of software systems and straightforward and common-use processing, which do not raise the same issues.

DISTINGUISHING BETWEEN CONCEPTS: ARTIFICIAL INTELLIGENCE SYSTEM (AIS) AND ALGORITHMS, TEACHER SYSTEM AND STUDENT SYSTEM

In the current public debate, AI is often assimilated to a particular category of algorithm, based on so-called learning techniques. The notions of AI and algorithm must, however, be distinguished, the algorithm being a technique used for the construction of AIS. Most AISs rely on one or more algorithms.

The algorithm is usually defined as a series of precise instructions allowing a result to be obtained from data provided as input.

5. In this sense, the historical definition used by Marvin Minsky makes artificial intelligence the science of making machines do what humans do with a certain intelligence (see in particular The Society of Mind, 1986). See also the definition used by the French Language Enrichment Commission in the Artificial Intelligence Vocabulary (list of terms, expressions and definitions adopted), published in JORF No. 0285 of 9 December 2018: "Theoretical and practical interdisciplinary field which aims to understand the mechanisms of cognition and reflection, and their imitation by a hardware and software device, for the purposes of assisting or replacing human activities.

6. For the European Parliament, artificial intelligence refers to the "possibility for a machine to reproduce behaviours linked to humans, such as reasoning, planning and creativity". (Website : Artificial intelligence: definition and use).

7. Depending on the notion of "intelligence" used, we sometimes distinguish between "strong" AI and "weak" or "moderate" AI. "Weak" or "moderate" AI systems refer to systems capable of performing very complex tasks thanks to their information management capacity. These systems rely on one of the components of human intelligence, cognitive power, to carry out the only functions for which they were designed, without consciousness or sensitivity. AI "strong" or "general" targets machines which would be endowed with a form of self-awareness and capable of carrying out an infinite number of tasks in a completely autonomous manner, thus imitating human cognition. Today it falls into the realm of pure science fiction; in the absence of a major technological breakthrough, current scientific advances do not allow us to envisage equipping a machine with all of human faculties.

The algorithms are very diverse. Schematically, they can be linked to two major conceptual categories of AIS, depending on whether they relate to symbolic (or cognitivist) AI or connectionist AI, i.e., one of the two major trends that appeared from the first work on AI in the 1950s.

Symbolic AI is a logical approach to information processing: any problem to be solved is broken down into a succession of simple and programmed logical actions so that a machine can carry them out quickly. Similarly to this approach, so-called teacher-system AISs, IT programs capable of solving complex problems through the application of precise rules by using a huge quantity of cutting-edge knowledge.

Connectionist AI is based on a probabilistic approach to information processing, and aims to enable machine "learning" using a huge quantity of data. The best-known application of this trend is machine learning (or "machine learning"), a technique consisting of building algorithms that "learn" on their own, that is to say, are capable of modifying their trainable parameters themselves in order to obtain the best performance. Also part of this trend are so-called "generative" artificial intelligence systems, capable of produce new original content from data used for their learning.

The concept of "artificial neural networks" is sometimes used to describe AISs based on a connectionist approach, in particular when it comes to "deep learning", an automatic learning process with many parameters (several layers of artificial neural networks).

In practice, the most common classification chosen by AI processes distinguishes between "**teacher**" systems and "**student**" systems.

AISs often combine algorithms from these two approaches.

The last ten years have been marked by the impressive growth of AIS thanks to access to massive volumes of data enabled by information and communication technologies, and the development of the computing power of digital tools. Beyond the contrasting feelings, enthusiasm or concern, that any technical revolution arouses, AISs are technologies of the present which are already disrupting the field of intelligence like all sectors of activity, calling for reinforced vigilance from the authorities of regulation and control.

1. AI is already widely used in the fields of defence and security, against a backdrop of incomplete legal framework

1.1. The surge in the use of artificial intelligence systems (AIS) in the fields of defence and security

1.1.1. The rise in the extent of their use in the field of defence and security, in particular for intelligence gathering

The field of security and defence is a privileged field of research and application in AI. The first historical developments in AI technologies focused on automated language processing (NLP) for defence purposes[8]. Intense research was carried out in the middle of the last century, particularly in the United States and the UK, aimed at creating machine translation programs, mainly in the English-Russian language pair. Benefiting from the support of American public authorities, this research met a war objective in order to translate captured Soviet communications.

Today, beyond the obvious use in the administration of defence and security forces (personnel management, logistics, maintenance, etc.), artificial intelligence processes are very present at the operational level, in the very implementation of security activities, in their many forms (automated information processing, human-machine interfaces, robotics, etc.).

8. This field of research was launched following the successes in decryption encountered during the Second World War and under the leadership of Warren Waever. This NLP pioneer proposed using computers to "decode" or " decipher" language in his famous memorandum, *Translation*, published in 1949. The approach took off in the 1950s.

There is no exhaustive inventory of all the cases of use of AIS by public authorities in charge of defence and security policies, but a few examples of recent developments help illustrate the usefulness and importance of these processes[9].

The **defence sector** is undoubtedly the one where the use of AI is the oldest and most intense. Today, the use of AIS in this area is very important for operational conduct, from combat support to weapon systems, the most sophisticated combat equipment all using one or more AIS.

In 2023, the possible use of "killer robots" sparked lively debates on the international scene given the risk posed by the removal of human control in the use of force[10]. Without going as far as this possibility of using an autonomous armed device without human supervision, automated weapon systems, possibly lethal[11], have existed for a long time and research to develop the autonomy of weapon systems has kept speeding up in recent years with the rise of AI learning methods (or "machine learning").

Although it appears more modest compared to the uses thus developed in terms of defence, the deployment of AI to carry out surveillance, public or secret, has accelerated in recent years.

Thus, **with regard to public security**, one of the most noted developments concerns the security of public spaces thanks to so-called "smart" (or "augmented") cameras, combining image recording devices (devices video protection, on-board or airborne cameras, etc.) to AISs analysing the resulting data flows to detect anomalies, suspicious behaviour or activities, or risky situations.

9. See in particular the study carried out by the Council of State at the request of the Prime Minister, Artificial Intelligence and public action: Building trust, Serving performance, adopted at the plenary general assembly on 31 March 2022, which includes a mapping of AI use cases, particularly in the fields of defence and security and investigation activities, control and sanction (Appendix 9).

10. In this regard, resolution 78/241 of the United Nations General Assembly, voted by 152 countries on 22 December 2023, notes that "the major issues and serious concerns raised by [...] the use of new applications technologies in the military field, including those linked to artificial intelligence and the autonomy of weapon systems", reflecting both the technical developments resulting from AI and the issues surrounding the new forms of weapons designated under the term of "lethal autonomous weapons systems" (or SALA).

11. Among these automated lethal weapons systems, there are for example anti-missile defence systems, whose technical success relies on AI, since the reaction time, in order to be usefully employed, excludes the use of human decision (other than in principle upstream, by activating the system), or even, more recently, armed drones such as the Predator and Reaper drones from the American company General Atomics Aeronautical Systems, some of which have been or are used in conflicts , particularly in the Middle East or Ukraine.

The law of 19 May 2023 relating to the 2024 Olympic and Paralympic Games[12] thus provides, on an experimental basis until 31 March 2025 and in the context of large-scale sporting, recreational or cultural events, that images collected by means of a video protection system or cameras installed on aircraft may be the subject of algorithmic processing in order to detect in real time and report certain predetermined events presenting or revealing risks of acts of terrorism or serious attacks on the safety of people. Excluded from this experiment are the most intrusive AISs, corresponding to algorithmic processing using biometric data[13/14].

However, if the use of public AISs using biometric data is currently prohibited, with the exception of authentication devices in the context of the processing of criminal records (TAJ) and the rapid crossing system at external borders (Parafe)[15],

AIS making it possible to identify natural persons thanks to biometric recognition processes, in particular facial recognition, which have undergone very significant progress in recent times and are widely used in the private sphere[16], are already experiencing significant uses in terms of security and preservation of public order in a number of countries (China and the United States in particular).

Likewise, **in terms of investigations and detection of offences**, AISs are increasingly used to enable the reporting of information, thanks to the widespread exploitation of the data flows that they authorise.

For example, since 2021, tax services have been experimenting with a new tool for collecting and using data publicly available online, for the purposes of detecting certain tax offences[17]. The exploitation and cross-referencing of data ("data mining"[18]) made possible by AI technologies allows the general directorate of public finances to identify fraud profiles by analysing and cross-referencing, through algorithms, all the information it has.

12. See Article 10 of Law no. 2023-380 of 19 May 2023 relating to the 2024 Olympic and Paralympic Games and containing various other provisions.
13. These are the physical, physiological or behavioural characteristics of a natural person which allow or confirm their unique identification.
14. See decision 2023-850 DC of 17 May 2023 of the Constitutional Council, recital 42.
15. Two experiments were also carried out on video surveillance devices with facial recognition during the Nice carnival in 2019 and during a football match involving the Olympique de Marseille team in 2021.
16. For example for authentication purposes, such as for smartphone identification processes.
17. See Article 154 of 2020 Finance Law no. 2019-1479 of 28 December 2019 and the extension of the experiment until 31 December 2026 set by Article 112 of 2024 Finance Law no. 2023-1322 of 29 December 2023.
18. "Data mining" would be at the origin of 52% of tax audits in 2022.

SOME CONCEPTIONS TO KNOW

Data mining: The process of automatically searching and exploring large amounts of data to discover trends and patterns that go beyond simple analysis.

OSINT (or open source intelligence): acronym for Open Source Intelligence, this notion refers, in terms of security, to a method of collecting and analysing information based on open access information and data.

In terms of digital defence, surveillance of cyber space has been significantly strengthened in recent years, alongside the observation of the importance taken by social networks in the process of manufacturing and disseminating information and the multiplication information manipulation operations carried out by foreign organizations or states. In this regard, the French authorities created the Viginum service in 2021, whose mission is to detect and characterise foreign digital interference affecting digital public debate in France, particularly during electoral periods. To carry out its surveillance, this service uses algorithmic processes to collect and process data from content publicly accessible on the online platforms on which it is authorized to investigate.

The intelligence-gathering techniques governed by Book VIII of the French Internal Security Code do not escape the development of the use of AIS both at the data collection stage and at the stage of their pre-exploitation or exploitation..

It is essentially for the exploitation and technical analysis of the data collected by the sensors that the use of AIS has become essential, the volumes concerned no longer allowing humans to carry out their exhaustive processing without machines. Automated big data management and processing technologies are thus used to organize and explore data stocks, ensure pre-processing and facilitate analysis. AISs therefore constitute processes supporting the implementation of some of the intelligence-gathering techniques provided for by the French Internal Security Code.

EXAMPLES OF AIS USE BY INTELLIGENCE SERVICES

"NL" software: automatic language processing tools aim to analyse, interpret and synthesize text in order to extract knowledge without human intervention, for a wide variety of applications - from instant translation of conversations or texts into another language to strategic intelligence operations. The Systran group, a French pioneer and world leader in automatic translation technologies, is a service provider for several intelligence agencies.

Preligens software: software from this company, specializing in geo-intelligence, ensures the automated processing and exploitation of large masses of data, particularly satellite data, for the benefit of French joint intelligence. They make it possible, for example, to identify abnormal movements on sensitive sites, to detect and count combat vehicles in conflict zones, or to map unknown places.

Furthermore, although this technique cannot be assimilated to an AIS, the French Internal Security Code authorises the use of algorithms "for the sole purposes of preventing terrorism"[19]. This intelligence-gathering technique, tested from 2015 then perpetuated by the law of 30 July 2021 relating to the prevention of acts of terrorism and intelligence[20], aims to enable the detection of terrorist threats based on the exploitation of data passing through the networks of electronic communications operators and Internet service providers. The five currently authorised algorithms[21] rely on artificial intelligence processes to analyse a significant amount of data according to predefined criteria, with worrying connections then being able to give rise to targeted checks by means of the identification of the person in question and the collection of related connection data.

19. See the provisions of Article L. 851-3 of the French Internal Security Code.
20. See Articles 15 and 18 of Law no. 2021-998 of 30 July 2021 relating to the prevention of acts of terrorism and intelligence.
21. See point 1.2.1 of the activity report.

1.1.2. The growing use of AISs in intelligence matters appears inevitable: the quest for efficiency

The growing use of AISs in the intelligence process appears essential to ensure its efficiency in the future in the face of three unavoidable constraints.

It arises first of all from a technical necessity in the face of "data revolution". The rise of AI occurs in a context marked by "datafication"[22] affecting all human activities and leading to exponential growth in data production so that with the human resources available, it is only possible to process a small - or soon to be a tiny part - part of the available data. AI therefore is an essential lever for controlling the digital world of tomorrow[23].

In the field of intelligence, the use of AISs is therefore essential to help service agents understand the huge quantity of data, browse it and better exploit it in order to be able to concentrate on the useful analysis of the elements available and guarantee the effectiveness of their intervention. The National Commission for Information Technology and Liberties (CNIL) thus summarises the consubstantial links maintained by data and machine learning AISs using the formula "The algorithm without data is blind. Data without algorithms is speechless"[24].

The development of the use of AIS is not only a technical response to the digital revolution. It also results from a necessary adaptation of the action of intelligence services to new forms of threats.

Since the beginning of the century, threats have in fact greatly diversified and no longer result solely from state adversaries fighting using traditional armed forces.

22. Term introduced in 2013 by Kenneth Cukier and Victor Mayer-Schöenberger in their essay, *The rise of big data*. "Datafier" a phenomenon aims to transform it into quantified, tabulated and analysable data.

23. As the mission led by Cédric Villani on artificial intelligence concludes, AI technologies "determine our capacity to organize knowledge, to give it meaning, to increase our faculties for decision-making and control of systems". See the Making Sense of Artificial Intelligence report. For a national and European strategy, published on 28 March 2018.

24. CNIL, summary of the public debate, How to allow man to keep control? The ethical issues of algorithms and artificial intelligence, 15 December 2017

A terrorist movement with global ramifications has thus developed, generating a disseminated and protean threat, calling for automation and extensive generalization of surveillance processes.

Likewise, the possibilities offered by the growth of the Internet and new digital communication tools allow our enemies to network their actions, to better conceal them and to circumvent surveillance. "Telephone tapping" which used to be the standard monitoring technique thus became much less productive due to the massive use of encrypted messaging and applications. Other techniques, although more recent, also come up against technological developments which question their effectiveness. The use of AISs appears in this context as a necessary tool to increase, or at least preserve, the effectiveness of legal intelligence-gathering techniques.

Furthermore, public authorities are today confronted with new forms of crime and new forms of conflict developing in cyberspace. Both "petty" delinquency and organized crime have found ways to facilitate their action as well as new criminal and criminal opportunities (online scams, cyberattacks, in particular). State powers or related organizations have also found a new fighting ground, making it possible to engage in informational struggles or attempts at destabilization.

The ability to have competitive AISs therefore appears decisive for maintaining the information, intervention and analysis capabilities of intelligence services in the face of the diversification of risks and threats, including technological ones, and avoiding any asymmetry between their means and those of enemies. The growth in the use of AI in intelligence is therefore essential to preserve both the defensive (detection of attacks, threats, crimes or offenses) and offensive (responses) capabilities of the State. In a context of marked international competition for the development and mastery of AI processes, a withdrawal of national services in this area would ultimately pose the risk of a loss of sovereignty.

1.2. The deployment of AISs is taking place against a backdrop of incomplete legal framework

Even though the use of AIS is expected to expand, AI regulation remains in its infancy today on the international scene as well as at the national level.

1.2.1. The profusion of thoughts and flexible rules of law when faced with the risks inherent in the deployment of AISs...

Between enthusiasm at recent achievements and the expected benefits of new "smart" digital tools on an economic and societal level and fear of human enslavement by machines or generalised surveillance, the rise of AI questions some of the major principles and balances that underpin democratic life.

These questions and concerns have translated over the last decade into a proliferation of reflections on the risks inherent to its development. In response, initiatives, public or private, aimed at defining an ethical framework for artificial intelligence or establishing guiding principles applicable in this area have multiplied.

Proposals for a charter, guide, or other recommendations, coming from state actors, international organisations, academic and research institutions but also from companies[25] or personalities[26], highlighting the issues inherent to the development of AI and setting out major ethical principles, are too numerous to be listed. At most, we can highlight **a movement tending to lay the foundations for international governance of artificial intelligence, by means of the adoption of a specific "ethics".**

25. See in particular the "Partnership for artificial intelligence for the benefit of citizens and society" concluded in September 2016 between Google, Facebook, IBM, Microsoft and Amazon to define good practices, particularly in terms of ethics, in the field. of AI, or the AI Ethics Charter adopted and published by Google in 2018.

26. From the scientific world in particular. For example, more than two thousand prominent people, including Stephen Hawking and Elon Musk, adopted at the end of a conference organised in January 2017, in Asilomar (California), a "*Reference guide for ethical development of artificial intelligence*", laying down 23 fundamental principles intended to legislate this development.

At the international level, this movement led in particular to the adoption of several proposed recommendations or charters, without binding legal scope, formalising the agreement of various States on the recommended uses, or conversely to be banned, of the AI.

The culmination of this movement, the Secretary-General of the United Nations announced in November 2023 the creation of a new advisory body on AI to support the efforts of the international community aimed at governing this new technology, emphasizing the need for organise "a global, multidisciplinary and multi-stakeholder conversation on the risks and challenges, opportunities and governance of AI" and the imperative for global regulation of emerging AI technologies based on the fundamental principles of the Charter of the United Nations and full respect for human rights.

THE MAIN NON-BINDING TEXTS ADOPTED AT THE INTERNATIONAL LEVEL

The Bletchley Declaration[27] for responsible AI: signed on 1 November 2023 in the United Kingdom by 28 states (including the United States, members of the European Union and China), this declaration formalises the agreement of participating countries to work together to establish a framework to ensure that AI technologies are developed and used responsibly and safely, "human-centred", and that the risks potentially "catastrophes" resulting from progress in this area are contained. This text is the most recent international cooperation initiative calling for framing the challenges and opportunities presented by AI.

The guiding principles and the voluntary code of good conduct of the G7 countries: this text, adopted on 30 October 2023 by the leaders of the G7 countries, sets general principles and lists 11 non-binding recommendations applicable to organisations which develop systems of Advanced AI, aiming at the development of "safe, secure and trustworthy" AI.

27. Bletchley Park is a former base of the English office responsible for the interception and deciphering of foreign espionage communications (Government Code and Cypher School) where Alan Turing and the decryptors who mastered the Enigma machine officiated.

The UNESCO Recommendation on the Ethics of AI: adopted on 23 November 2021 by the 193 UNESCO Member States meeting in the General Conference, this recommendation recalls the imperative of protecting human rights and the dignity of the human person, calls for respect in the deployment of AI of fundamental principles such as transparency and fairness, and establishes the importance of human responsibility in the control of artificial intelligence systems. It invites Member States to take appropriate measures, in particular legislative measures, to guarantee compliance with the principles and standards it sets out.

The OECD Recommendation on Artificial Intelligence: this recommendation, adopted by the OECD Council on 22 May 2019 and amended on 8 November 2023, acknowledges that "AI promises to improve prosperity and well-being be individuals, to contribute to dynamic and sustainable global economic activity, to stimulate innovation and productivity, and to help confront major global challenges", **while admitting that its development puts** "democracy and human rights, privacy and data confidentiality, and digital security **to the test." It sets out the principles of a responsible approach in support of trustworthy AI, specifying that AI actors should in particular "respect the rule of law, human rights and democratic values throughout of the life cycle of AI systems"** and commit to ensuring the transparency and explainability of their AIS.

At the European and French levels, ethical and legal reflections and regulatory proposals have been equally abundant for several years.

In June 2019, the Council of Europe set up a Committee on Artificial Intelligence[28], tasked by the Committee of Ministers with developing a framework convention on the development, design and application of artificial intelligence. artificial intelligence, based on Council of Europe standards on human rights, democracy and the rule of law. The first reflections of this group on the principles of a legal framework for artificial intelligence were published in December 2021[29].

28. Ad hoc Committee on Artificial Intelligence (CAHAI), replaced in 2021 by the Committee on Artificial Intelligence (CAI).

29. Report on "Potential elements of a legal framework on artificial intelligence, based on Council of Europe standards on human rights, democracy and the rule of law".

The European Union had initiated reflections on artificial intelligence with the adoption as early as April 2018 of its communication on *Artificial Intelligence for Europe*, announcing a coordinated plan on artificial intelligence, immediately followed by the setting up of an advisory board made up of 52 independent experts, The Group of independent experts in artificial intelligence[30] whose mission is to provide expertise, strategic advice and proposals to develop "trustworthy artificial intelligence". The work of this group[31], whose mandate came to an end in July 2020, notably served as resources for initiatives to develop the digital policy of the European Union, as well as for the development of legislation in this area of AI, adopted on 21 May 2024 (see point 1.2.2 below).

Concerning more specifically the study of the impacts of AI on the guarantee of rights, the Fundamental Rights Agency, responsible for providing assistance in this area to the EU institutions and authorities, has published several studies analysing its impact on rights and freedoms, in particular the risks of facial recognition and the bias and discrimination generated by algorithms[32] and proposing guidelines to be retained.

In France, public reflections are also very abundant. Numerous reports and studies examining the issues surrounding the rise of AI have followed one another over the last decade, with discussions mainly focused on ethical and, to a lesser extent, legal issues. Proof of this priority given to ethical considerations are the proposals from the Parliamentary Office for the Evaluation of Scientific and Technological Choices on AI submitted in March 2017[33], the CNIL study on the ethical issues of algorithms and intelligence artificial intelligence of December 2017[34] and Cédric Villani's report of March 2018[35], which paved the way for the launch of the *national strategy for artificial intelligence* at the end of 2018.

30. GEHN IA, or High Level Group on Artificial Intelligence, AI HLEG.

31. See in particular the *Ethical Guidelines for Trustworthy AI* report, published on 8 April 2019.

32. Reports entitled *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 November 2019 and *Bias in algorithms - Artificial intelligence and discrimination*, 8 December 2022.

33. Report No. 464, *For a controlled, useful and demystified artificial intelligence*, volume I, filed on 15 March 2017.

34. Mentioned above, note 24.

35. Mentioned above, note 23.

1.2.2. | ... contrasts with the lack of overall regulation on AI techniques in positive law

While recent years have seen a proliferation of soft law instruments, most often responding to concerns about the "ethical" use of AI, this technology has until now developed outside of any specific legal framework.

Certainly, general international, European or national instruments for the protection of fundamental rights are intended to apply to all areas of life, regardless of the technology used and therefore also to AIS.

As for France, the major principles, rights and freedoms enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter of Fundamental Rights of the European Union and the constitutionality bloc, in particular the right to respect for private life, freedom of expression and assembly, or even the principles of equality and non-discrimination, can govern the use of techniques using AI, in particular in their use by public authorities in the field of security. Some rules specifically applicable to AISs were thus able to be identified on the basis of these principles, particularly in terms of surveillance.

SOME EXAMPLES OF THE APPLICATION OF FUNDAMENTAL RIGHTS TO MONITORING AND INTELLIGENCE-GATHERING TECHNIQUES USING AIS IN EUROPEAN JURISPRUDENCE

Consequences of technological developments:

As early as 2008, the European Court of Human Rights (ECHR) clarified, in a case involving the collection and retention of biological data by public authorities for the purposes of crime prevention, that the use of modern scientific techniques shall necessarily be assessed with regard to a balancing of the advantages which could result from the use of these techniques and respect for the fundamental rights of individuals, in this case the essential

interests relating to the protection of privacy. Therefore, the State claiming the use of new technologies bears the particular responsibility of finding the right balance in this matter. In this case, the Court underlines that the high rate at which innovations in the field of genetics and information technologies are occurring creates risks of infringement of private life in new ways, which we do not can predict today with precision (CEDH, *S. and Marperc. United Kingdom*, No. 30562/04 and 30566/04, 4 December 2008).

Mass surveillance:

In a case relating to mass surveillance of communications, the ECHR examined the use by governments of cutting-edge technologies allowing them to intercept a very large amount of data, in order to fight against the new forms taken by terrorism. In this case, it censored the Hungarian regulations due to the disproportionate harm to the right to respect for private life that it allowed and the lack of any effective remedy (ECHR, 12 January 2016, Szabó and Vissy v. Hungary , **no. 37138/14**).

Subsequently, in two judgements of 25 May 2021, the Grand Chamber of the ECHR examined the conditions in which a regime of mass surveillance of electronic communications, which may include AI tools, is compatible with Articles 8 (right to respect for correspondence and private life) and 10 (freedom of expression) of the Convention (ECHR, 25 May 2021, Big Brother Watch and others v. United Kingdom, nos. 58170/ 13, 62322/14 and 24960/15, and 25 May 2021, Centrum för Rättvisa v. Sweden, no. 35252/08).

Facial recognition:

In a case relating to the indefinite conservation of personal data (DNA profile, fingerprints and photographs), the ECHR notes that the rapid development of increasingly sophisticated techniques allowing, among other things, facial recognition or mapping from photographs of individuals, makes the capture of their image and the conservation of the data collected problematic. It emphasizes that the complex nature of the technologies used shall be taken into account when examining the necessity of interference in the right to respect for privacy of the individual whose image was captured (ECHR, 13 February 2020, Gaughran v. United Kingdom, no. 45245/15).

Apart from the application of these general instruments protecting fundamental rights and freedoms, the use of AISs is not currently governed by any specific general regulations. The development of the latter is thus only governed, in European law as in national law, by scattered provisions enacted in other matters.

With regard to the European Union, it is however worth noting the recent adoption of legislation aimed at specifically regulating artificial intelligence, the draft AI Act. Based on a legislative proposal presented by the European Commission on 21 April 2021, a provisional agreement between the Council and the European Parliament was reached on 9 December 2023 on a draft regulation setting out harmonised rules regarding artificial intelligence and aiming, at the same time, to stimulate investment and innovation in this area and to supervise AI systems to ensure the proper functioning of the internal market and guarantee high standards in terms of ethics and respect for fundamental rights. The AI ACT project was adopted by the European Parliament on 13 March 2024 and by the European Council on 21 May.

This project, whose scope of application is very broad due to an encompassing definition of artificial intelligence systems and the narrowness of the areas of exclusion, adopts a risk-based approach leading to banning AISs presenting a risk unacceptable, to impose strong constraints on high-risk AIS and to subject other systems to only light obligations. The rules adopted for the various AISs are accompanied by the setting up of a revised system of governance and specific sanction mechanisms in the event of violation of the legislation.

The regulation **establishing harmonised rules on artificial intelligence** (AI Act), scheduled to enter into force in 2026, will be one of the first general laws applicable on AI in the world with that recently implemented in United States[36].

36. With the passing of the National Artificial Intelligence Initiative Act (NAIIA) in 2020 and the Presidential Executive Order Safe, Secure, and Trustworthy Artificial Intelligence in October 2023.

OUTLINE OF THE REGULATION ESTABLISHING HARMONIZED RULES CONCERNING ARTIFICIAL INTELLIGENCE (AI ACT) ADOPTED BY THE EUROPEAN PARLIAMENT AND THE COUNCIL

Scope

The regulation, which will be fully applicable in 2026, retains a fairly broad definition of the techniques it is intended to regulate. It defines the artificial intelligence system as "*an automated system designed to operate at different levels of autonomy, which can demonstrate a capacity for adaptation after its deployment and which, for explicit or implicit objectives, infers, at from the input data it receives, how to generate results such as predictions, content, recommendations or decisions that can influence physical or virtual environments*" (Art. 3 (1) of chapter I[37]).

The regulation is intended to apply to all AIS placed on the market or put into service in the Union, or used by a user present or established in the Union, and lays down specific obligations for suppliers (developers) or users ("deployers") of AI systems. However, it will not apply to AI systems used for military, defence or national security purposes, as these areas fall outside the scope of EU law. It will not affect the competences of the Member States in matters of national security, whatever the type of entity entrusted by the Member States with carrying out tasks linked to these competences (art. 2.3 of Chapter I[38]). It will also not be intended to govern systems used solely for the purposes of research and innovation (art. 2.6 of Chapter I).

Classification of AI systems:

The regulation classifies AISs according to the risks they present:

Banned AISs (Art. 5 of Chapter II[39]):

The text plans to ban AISs presenting an unacceptable risk. Considered a clear threat to the fundamental rights of individuals, the following practices, whether intentional or not, are prohibited: techniques relating to cognitive behavioural manipulation; methods exploiting vulnerabilities linked to age,

37. As per provisional numbering available when this report was printed.
38. As per provisional numbering available when this report was printed.
39. As per provisional numbering available when this report was printed.

disability, or economic or social situation; social rating methods evaluating or classifying individuals or groups on the basis of their social behaviour or personal traits; assessing the risk that a person commits criminal offenses on the sole basis of profiling or personality traits, unless there are limited exceptions; the creation of facial recognition databases by non-targeted extraction of facial images on the internet or video surveillance images and remote biometric identification in real time in public places, subject to the exceptions determined by the regulation for their use by law enforcement.

High-risk AISs (Chapter III[40]):

This category brings together systems used in listed industrial sectors (notably civil aviation, transport, etc.) or identified as being inherently high-risk and listed in the appendix (notably biometric systems and systems supporting law enforcement authorities). Also classified as high risk are AISs that establish person profiles (automated processing of personal data used to assess various aspects of a person's life, such as their professional performance, their economic situation or, their health, in particular).

The placing on the market or in service and the use of these high-risk AISs is governed by specific obligations meant to guarantee their reliability and safety, particularly in terms of human control of the machine, establishment of documentation technical, implementation of a risk management system. Additionally, a fundamental rights impact assessment must be carried out before a high-risk AI system is placed on the market.

General Purpose AI (GPAI) models:

The Regulation provides a special regime for GPAIs, which are characterized by their high generality and their ability to competently perform a wide range of distinct tasks, regardless of how the model is placed on the market, and which can be integrated in a variety of downstream systems or applications. These models must comply with specific transparency obligations before being placed on the market, with stricter rules provided for those of these models which are considered systemic, including an assessment of systemic risks and an obligation to protect cyber security.

40. As per provisional numbering available when this report was printed.

The other AISs:

AI systems that present minimal risk are not subject to any specific obligations under the Regulation, apart from a light transparency obligation.

Governance:

The text provides in particular for the creation of an AI Office (or AI Office) within the European Commission and a European Artificial Intelligence Committee bringing together state representatives and the European Data Protection Supervisor as an observer. It further includes rules regarding the designation of competent national authorities, including a "notifying" authority and market surveillance authorities, to ensure the implementation of the regulation. These authorities will have the particular mission of representing the Member State within the European AI Committee, of accrediting and evaluating compliance bodies and of ensuring the proper functioning of the AIS market.

However, apart from the fact that the AI Act will not apply as a whole before 2026, this new regulation will not cover all the subjects raised by the increased use of AISs in the field of public action. In particular, it will not apply to matters of intelligence due to the exclusion of the areas of defence and national security from its scope of application.

In fact, the framework currently applicable to AISs results from the juxtaposition of various rules, the overall consistency of which remains to be built.

Apart from higher, constitutional or conventional standards, requiring respect for fundamental rights and freedoms, the provisions applicable to AISs fall under sectoral legislation which concerns its hardware components (software, equipment, etc.) or certain of the processes used (data processing, algorithm, etc.).

On this second aspect, the most sensitive, AISs are essentially concerned by the regulations relating to the **processing of personal data**[41].

41. For an exhaustive presentation, see Appendix 10 of the aforementioned study by the Council of State, note 9.

Any AIS using personal data is thus considered **processing of personal data** within the meaning of Law No. 78-17 of 6 January 1978 relating to data processing, files and freedoms, which specifies in its first article that: "*IT must be at the service of every citizen. [...]. It must not infringe on human identity, human rights, private life, or individual or public freedoms*". AISs must respect the rights granted to individuals to access personal data concerning them, to have them rectified and to file an objection set out, as the case may be, by the general data protection regulation (GDPR)[42], by Title III of the law of 6 January 1978 for processing covered by the so-called police-justice directive[43], and by Title IV of the said law for processing not falling within the scope of Union law, in particular those who concern the defence and security of the State, like the processing used by the intelligence services.

Furthermore, when public systems are involved, a body of rules also applies to ensure the **transparency of public action**. Two devices are mainly concerned.

First of all, in application of the code of relations between the public and the administration, users benefit from a general right of access to administrative documents, which allows them to request communication of the structuring elements of the AIS such as files, source codes, or the completed technical documentation relating to an AIS used within the framework of a public service mission.

Then, the GDPR, the law of 6 January 1978 and the code of relations between the public and the administration provided for specific follow-up of administrative decisions based on algorithmic processing - qualified as "automated decisions" - when they are issued on the sole basis of such processing. In this regard, Article 47 of the Law prohibits in principle that a decision which produces legal effects with regard to a person or significantly affects them is taken on the sole basis of automated

42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

43. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention and detection of criminal offences, investigations and prosecutions in this matter or execution of criminal sanctions, and the free circulation of this data

processing, except, in particular, if it is an individual administrative decision, said decision shall then mention that it was based on algorithmic processing. Such a possibility is excluded for decisions falling within the scope of the police-justice directive if it is not surrounded by appropriate guarantees, and at least the right to obtain human intervention. The code of relations between the public and the administration provides for enhanced information for users when a decision based on algorithmic processing is in question, whether in the presence of an "automated decision" or simply 'a decision assisted by treatment[44].

Finally, the code of relations between the public and the administration requires administrations of more than 50 agents to publish online, spontaneously, the rules defining the main algorithmic processing used in the accomplishment of their missions when they base individual decisions[45].

With regard more specifically to intelligence, the legal framework for used AISs also appears limited.

On the one hand, with regard to the processing of personal data, the techniques used in the field of intelligence in fact fall under a derogatory regime providing, at best, only indirect access to the personal data contained in files concerning state security, defence or public security[46] it being specified that they are also outside the scope of application of the GDPR and the police-justice directive. Regarding the obligations of transparency of public action, they are obviously excluded for secret surveillance, given their very purpose.

On the other hand, the use of artificial intelligence is not specifically regulated by Book VIII of the French Internal Security Code, which, apart from the consecration of a particular use of the algorithm in its Article L 851-3 (see point 1.1 above), only incidentally mentions artificial intelligence-gathering techniques.

44. Such a decision must include mention of the fact that it was taken on the basis of algorithmic processing and the administration is required, in the event of a request from the interested party, to communicate to them, in an intelligible form, the rules defining this processing and the main features of its implementation

45. See Article L. 312-1-3 of the CRPA.

46. The guarantees provided by the general regime of the right of access and rectification are in fact incompatible with so-called "sovereignty" treatments.

Only Article L. 854-2 thus expressly mentions the possibility for intelligence services to implement automated processing, for the exploitation of connection data intercepted in the context of international surveillance. It should nevertheless be considered that III of Article L. 822-2 of the French Internal Security Code, by authorising "research programs", aims to enable the use of AI tools for research and development needs in terms of techniques for collecting and using information[47].

In the absence of a precise legal framework, the use of AI in intelligence matters requires delicate work of interpreting existing legal principles and rules, enacted without taking into account the specific issues raised by technological developments.

2. The challenges raised by the speeding up of AIS use in the field of intelligence gathering call for particular vigilance and reinforced control

2.1. Specific risks and challenges in the field of intelligence

The use of AIS in matters of national security, and particularly in the field of intelligence, raises major ethical questions and specific issues that must be limited.

47. It appears from the parliamentary debates that the introduction, by Article 10 of law no. 2021-998 of 30 July 2021, of these provisions derogating from the general rules of data retention resulted from taking into account the needs of data artificial intelligence tools, in particular algorithms (see in particular on this point the report of senators Mr Marc-Philippe Daubresse and Ms Agnès Canayer, No. 694 of 16 June 2021).

2.1.1. | Risks linked to automation

The growth in the use of AI in the field of security and public order regularly resurfaces the fear of mass surveillance of the population by public authorities.

AI is fundamentally based on automation, which has the function of optimizing and accelerating a process by replacing humans. Today, automation technologies enable the massive and rapid capture and use of data. If we add the fact that the most recent AI tools can be used mobile and interconnected, widespread surveillance of populations seems within reach.

Therefore, the use of new technologies in security matters can be seen, not as a factor in promoting collective security, but as an instrument of mass surveillance, a feeling fuelled by the distrust felt by part of the population towards -vis the State and its sovereign functions.

The practices of certain governments have, it is true, demonstrated the capabilities of new surveillance technologies. Emblematic in this area, the Chinese communist regime has developed an unprecedented project for surveillance of its citizens, relying in particular on the deployment of a social credit system, a device for permanent control of individuals based on artificial intelligence and "Big Data".

Without falling into fear of the widespread reproduction of such a model, the multiplication of surveillance that automation allows nevertheless inherently carries a major risk of infringement of the right to respect for private life, in particular the protection of personal data, and indirectly threatens freedom of expression through the phenomenon of self-censorship that the deployment of surveillance devices can generate, thus influencing the behaviour and psychological balance of individuals ("chilling effect"). If most of the AISs developed have

neither the aim nor the effect of modifying the conditions in which the data is collected, they in fact allow a systematic and automated analysis of the latter likely to considerably increase the number and precision of the information which can be extracted.

Another consequence of automation, alongside the increase in monitoring possibilities, the loss of human control is often highlighted to highlight the dangers of AIS.

One of the most essential questions raised by the use of AI tools relates to the consequences of delegating critical decision-making to a "machine" or even the massive delegation of non-critical decisions.

In this regard, the emphasis is first placed on the risk of disempowerment of the "decision-making" agent, as well as on the biases introduced into his decision, AISs being never neutral since they are configured by the man by inevitably incorporating bias.

Such a difficulty arises in the field of intelligence as in the rest of the field of public action, however with particular acuteness due to the sensitivity of the matter. Apart from the particular case of the algorithm technique, the legal framework for the implementation of intelligence-gathering techniques is in fact focused on the human exploitation of the data collected and thus places the responsibility of verifying the public interest purpose pursued, the justified nature of surveillance and the proportionality of the interference in fundamental rights and freedoms to the threat or issues in question.

The use of AIS tools, fast and powerful, may raise fears that the technologies are not just a simple aid to decision-making but replace the agent in his task, the latter limiting himself to ratifying the results proposed by the machine. A hiatus could therefore emerge between a perceived responsibility of the agent and his/her legal responsibility, in particular criminal, as set by Article L. 862-2 of the French Internal Security Code.

In addition, the loss of human control takes on a particular dimension with the developments of generative AI. Indeed, AISs based on deep learning processes or even only on particularly complex algorithms are characterised by their opacity.

These AISs can quickly prove too complicated to be presented and understood by the agents responsible for using them. Beyond these agents, the opacity of AIS represents a particular challenge for the people and authorities responsible for controlling them. It could even question the right to effective legal recourse, which requires an understanding sufficient use of technologies by the jurisdictional authority to enable the rendering of a fair decision.

The ability to explain[48] the functioning of systems today constitutes one of the major challenges associated with the rise of AI and raises the question of control and the possibility of auditing the surveillance processes implemented.

2.1.2. Challenges specific to data management and consistency of the legal framework

The development of the use of AIS by intelligence services raises two specific issues relating to data management and the coherence of the legal framework in force.

The deployment of AISs questions the data management principles defined by the law-maker in order to preserve the balance between the necessities of public interest covered by the public policy on intelligence and the protection of human rights and fundamental freedoms, particularly privacy protection.

To ensure this balance, the provisions in force of the French Internal Security Code strictly determine the terms of use of data collected by

48. See in particular the analysis concerning learning AI in the aforementioned Villani report, see note 23.

the intelligence services, including in the context of research and development, set the retention periods of each type of data, regulate their possibility of sharing, within and outside the intelligence community, and limit the possibilities of crossing different administrative police files.

However, the massive, shared and cross-use of data is consubstantial with the development of machine learning AI. AISs are in fact all the more efficient when they are fed by a large set of data, of varied nature, and that they can process them without any particular condition or time limitation. The provision of mass data deposits to digital players is also one of the considerations which led to the adoption, at European level, of a legislative package relating to data governance, made up of a regulation on data governance (Data Governance Act) and a regulation on data (Data Act)[49]. Intended to promote responsible access, sharing and reuse, in compliance with the values of the European Union, of data (open data, public sector information, or personal data), this legislation establishes an environment presented as necessary for the success of the European strategy in terms of artificial intelligence.

THE MAIN PRINCIPLES OF DATA REGULATIONS

The regulation on data governance, applicable since 24 September 2023, and the regulation on harmonised rules on fair access and use of data, which will be applicable from 12 September 2025, set the European strategy on the data. They aim to strengthen the EU's competitiveness and sovereignty in this area by defining a harmonized framework enabling economic actors and EU Member States to harness the potential of data and foster innovation.

These texts therefore aim to promote access, sharing and reuse of data in Europe, in compliance with EU law – in particular the rules for the protection of personal data set by the GDPR.

49. See Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [Data Governance Regulation] and Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 concerning harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [data regulation].

In particular, they lay down the principles:

- fairness between economic actors in the use of data generated by connected objects;

- the possibility for companies to reuse data held by public sector bodies, including so-called data "protected" after anonymization;

- access of public sector organizations to private data, in the event of exceptional needs;

- setting rules to facilitate the flow of data between service providers and data processing companies.

The rules laid down by the French Internal Security Code, which tend to minimize both the collection of data and their possibilities for conservation and sharing, can thus come into tension with the needs of AI in its possible applications in terms of intelligence.

In this regard, two particular difficulties or questions can be highlighted.

First of all, the development of AI questions the scope and relevance of data retention rules in that they are based on the distinction between "collected information", raw data collected, and "transcriptions" or "extractions", worked data. However, the use of AISs in intelligence-gathering devices or in data management tools can blur these distinctions. AISs based on self-learning techniques raise new questions in this regard by creating a new category of data, data incremented in the model itself. Since the raw data input into the AIS is incorporated into the system, determining a retention period other than the duration of use of the AIS makes less sense.

Then, the development of AI is likely to undermine the relevance of the durations chosen with regard to the operating difficulties it generates for the services. This is the case, for example, new encryption and cryptography possibilities that make data analysis more difficult and time-consuming. It is moreover this consideration which led

the law-maker to introduce exceptional retention periods for information containing elements of cyber-attack or encrypted[50]. A similar concern also resulted in the introduction in 2021 of longer data retention periods to allow the development, improvement and validation of technical collection and exploitation devices, the legislator having taken into account the needs in data necessary for the development of artificial intelligence tools[51]. This exemption is in line with regulations, such as the European AI Act, which provide for the establishment of regulatory "sandboxes" consisting of creating a specific legal framework for the development, testing and validation of innovative systems.

Finally, it should be noted that the legal framework in force is largely built on the principle of human exploitation of intelligence, by natural persons, individually designated and authorized agents, without taking into consideration the intervention of machines.

In addition to the perception of data, the rising use of AISs also questions some of the essential distinctions and boundaries set by current regulations.

First of all, the question arises of the very determination of regulated intelligence techniques, while Book VIII of the French Internal Security Code bases intelligence law on an approach by intelligence-gathering technique and not by operation or by target. The development of AISs indeed leads us to question the possible emergence of new regulated techniques in correlation with the technological progress made, an evolution which presupposes first distinguishing, among the systems presenting an interest in surveillance, those which must be established as intelligence-gathering techniques of those which should only be regarded as simple processes incorporated into a technique covered by the French Internal Security Code or into an exploitation tool.

50. See the provisions of Article L. 822-2 of the French Internal Security Code.

51. See III of article L. 822-2 of the French Internal Security Code resulting from article 10 of law 2021-998 of 30 July 2021, and report of senators Marc-Philippe Daubresse and Agnès Canayer, no. 694 of 16 June 2021, on the bill.

The rise of AI also raises questions about the fragmentation of legislation and governance in the areas of digital technology and data management. As explained above, the use of AI techniques is at the crossroads of different regulations and their regulation involves several authorities or control entities[52], raising the question of the consistency of the applicable rules. In terms of intelligence, technological developments have brought closer the means and processes used by the different actors in matters of public security and favoured a continuum of actions, making it more difficult to determine the boundary between public surveillance and secret surveillance and easier the possibilities, circumvention of the most restrictive legislation. Combined with the data revolution, they also encourage confusion between data processing and the exploitation of surveillance results.

2.2. ... that require extra vigilance and control

Within the framework of the margin of appreciation left to Member States by European legislation on AI, internal regulatory avenues have already been formulated to ensure a satisfactory balance between the development of a European ecosystem favourable to technological innovation and respect for fundamental rights and freedoms.

One of the most common recommendations consists of favouring, at least initially, a framework through flexible law in order to make easier to adapt to unpredictable technological developments. The use of AIS in very sensitive areas, particularly in security and defence, could however be subject to national regulation through stricter sectoral regulations.

Without waiting for such normative intervention, the development of AI in the field of intelligence calls for an evolution of control methods.

52. In particular, at the national level, the CNIL, the Regulatory Authority for Electronic Communications, Posts and Press Distribution (ARCEP), the Regulatory Authority for Audiovisual and Digital Communication (ARCOM) and the Interministerial Directorate of digital (DINUM).

Thus, in the absence of specific supervision, the use of AIS by services leads the supervisory authorities, including particularly the CNCTR, to identify, based on the existing legal corpus, the rules and principles to be complied with so that their employment respects fundamental rights and freedoms. While such an exercise remains usual for most control bodies, the guiding principles for the operation of AISs used for the most sensitive operations in the intelligence chain, such as the requirement to be able to explain processing, the need for control human nature of their results, or the imperative of robustness of the models deployed, which the Commission is already working to ensure compliance with, deserve to receive a legal basis. The same goes for the supervision of the use of AISs by the intelligence services, whose recognition as one of its full-fledged missions of the CNCTR would be a guarantee of confidence for citizens.

2.2.1. | Possible guarantees in the field of intelligence

The growth of AISs in fact reinforces the imperative of human and technical strengthening of the control capacities of the CNCTR[53] so that it is able, on the one hand, to cope with the increase in the number of authorized intelligence-gathering techniques and data collected by the services and, on the other, to assess the robustness and acceptability of the systems used to implement these techniques and exploit this data.

In the same way, it makes the developments recommended by the CNCTR in terms of centralisation of the data collected and remote access[54] to this data for control purposes even more crucial, given the risks and issues previously mentioned.

In the current normative context, it also leads to the development of a new modality of ex ante control through the formulation of guidelines or recommendations aimed, in the imprecision or silence of the French Internal Security Code, at ensuring the compatibility of the technologies used by the services with the general principles established by the texts.

53. See in particular the 7th 2022 CNCTR activity report, p. 56 and following.
54. See point 3.1 of the activity report.

This possibility, which can be included in the general prerogatives of formulating recommendations, observations and opinions recognized by the CNCTR by Articles L. 833-6, L. 833-10 and L. 833-11 of the French Internal Security Code, is an essential tool to prevent the development of the use of "black boxes" by services, the impact of which is little or poorly understood. It is in fact a way of applying prudential regulation to AI tools used in intelligence matters in the same spirit as that provided for high-risk AISs by European regulations, which requires suppliers to certify models and artificial intelligence applications.

In an approach similar to that established by the AI Act, this area of control consists, in view of the characteristics of the processes and algorithms offered by the services and the technical documentation transmitted, of auditing these tools and analysing their impact on legal principles and fundamental rights, then to recommend an employment doctrine. This focuses both on ensuring compliance with the general rules laid down by the French Internal Security Code and on ensuring that the principles necessary for the preservation of fundamental rights and freedoms, such as the imperative of human control, are taken into account on the results of AIS or the individualized nature of domestic surveillance.

The success of this approach requires that the effectiveness of this new area of control, which for the CNCTR is part of an approach of support and regulation through soft law, thus presupposes better transparency of services in terms of the tools deployed.

THE EUROPEAN PRINCIPLES FOR REGULATING HIGH-RISK AISS (AI ACT)

Strong obligations for the system supplier:

The supplier must in particular:

– put in place adequate risk assessment and mitigation systems (identification and analysis of known and foreseeable risks; estimation and evaluation of potential risks, adoption of appropriate risk management measures, etc.).

– ensure governance of the data feeding the system, ensuring that training, validation and test datasets are relevant, sufficiently representative, error-free and complete, in order to minimize risks and discriminatory results;

– provide detailed documentation including all the necessary information on the system and its purpose, to enable the authorities to assess its compliance;

– provide human control, in order to minimize risks;

– assume a high level of robustness, security and precision of the models.

A compliance review:

Before the high-risk AIS is put into service, the supplier must undergo a procedure to assess the conformity of the system with the obligations provided for by the regulation. For most AISs, the assessment is carried out as part of an internal control procedure, without intervention from an external body. For the riskiest AISs, the assessment must be carried out by an independent external authority.

2.2.2. Beyond mere intelligence, the challenge raised by consistent regulation for all monitoring techniques

The entry into force of European legislation on AI and the implementation of the various supervision mechanisms that it establishes will require the adoption of new digital governance.

Given the place occupied by personal data in issues relating to AI, the function of national supervisory authority responsible for the regulation of AISs could fall to the CNIL. This is notably the recommendation of two recent fact-finding missions from the Committee on Constitutional Laws, Legislation and Administration of the National Assembly[55] and the Committee on European Affairs of the Senate[56], a conclusion which agrees with the opinion of the CNIL itself and its European counterparts[57]. Furthermore, it can be noted that, with regard to the AISs of the Union institutions, European legislation entrusts the role of regulator to the European Data Protection Supervisor.

The market regulation role which would thus be entrusted to the CNIL would not, however, exhaust the control needs of AISs. Outside the scope of European legislation, AISs used in matters of national security and defence deserve specific regulation and supervision aimed at reconciling the preservation of individual rights and freedoms and the imperative of discretion, or even secrecy when involved information classified under national defence secrecy, which is required for the effectiveness of public action in these areas.

The various technologies contributing to national security and defence, which cover current practices, such as video surveillance of public places,

55. View the briefing report on behalf of the Business Committee the Committee on Constitutional Laws, Legislation and Administration on the challenges of generative artificial intelligence in relation to the protection of personal data and the use of generated content , by Messrs Pradal and Rambaud recorded on 14 February 2024.

56. See the information report on behalf of the European Affairs Committee relating to the proposed European legislation on artificial intelligence, by Mr André Gattolin, Ms Catherine Morin-Desailly, Mr Cyril Pellevat and Ms Elsa Schalck recorded on 30 March 2023.

57. Opinion of 18 June 2021 on the European Commission's proposed regulation on AI.

more recent methods, such as capturing images by drones or on-board cameras, up to particularly intrusive processes. represented by facial recognition technologies or certain secret intelligence-gathering techniques such as the collection of computer data, today fall under fragmented controls, carried out by authorities of various kinds, without general supervision. However, public security and intelligence policies translate in this area into a continuum of actions and are similar in the techniques used.

Close supervision and coordinated control of the use of these new technologies by security forces, guaranteeing use proportionate to the needs of collective security without instrumentation for mass surveillance, would be a guarantee of their effectiveness and social acceptability.

Insight 2. Responsible use commercial cyber intrusion capabilities: a diplomatic perspective

Contribution from Mr Henri Verdier, the French Ambassador for Digital Affairs, and Mr Léonard Rolland, the Cybersecurity Officer, Sub-Directorate for Strategic Affairs and Cybersecurity, Ministry of Europe and Foreign Affairs

For a quarter of a century, in response to the challenges brought about by the appearance of a new space of digital conflict, States have negotiated at the UN, as well as within ad hoc diplomatic formats, the parameters of what they consider to be "responsible behaviour" in cyberspace, and in particular "responsible use" of cyber capabilities.

Some of these capabilities, such as cyber-intrusion tools, can be used legitimately by intelligence services and internal security forces within a strict legal framework, for administrative or judicial investigations under the control of the CNCTR. or a magistrate. In parallel with these legitimate uses, a market for intrusion capabilities has developed in recent years, driven by private companies selling to the highest bidders. These capabilities are then likely to be used in conditions that guarantee neither respect for human rights nor the stability and security of cyberspace.

Faced with the risks arising from the proliferation and irresponsible use of offensive digital tools, it is therefore necessary to adopt an approach and governance capable of defining roles and responsibilities respective states and the private sector. It is in this spirit that the Paris Call launched by the President of the Republic in 2018, and supported by a large number of States and companies, wished to add this subject to the agenda of our international discussions. The Appeal then affirmed

that the fight against the proliferation of malicious software and computer practices intended to cause harm constituted a principle in its own right to ensure trust and security in cyberspace.

This phenomenon of cyber proliferation by private actors has recently been the subject of an ad hoc diplomatic initiative. In February 2024, France and the United Kingdom jointly launched the Pall Mall Process, a long-term diplomatic process aimed at combating the proliferation and irresponsible use of available cyber-intrusion capabilities in the market. At the heart of our diplomatic work, the notion of "responsible use" of such capabilities by States, which will need to be the subject of significant definition work. Likewise, the initiative aims to identify and promote "good practices" in terms of controlling this use. In this context, France will naturally be led to promote its national approach and practices, including the control work carried out by the CNCTR.

The challenge of the emergence of a cyber intrusion market

In a declaration adopted on the occasion of the launch of the Pall Mall process in February 2024, a coalition made up of States, businesses, and representatives of civil society emphasized with regard to the cyber-intrusion market that "this growing market, with its transformational effects on the cyber landscape, significantly expands the potential group of state and non-state actors with access to commercial cyber intrusion capabilities, increases the risks of malicious and irresponsible uses and makes more difficult to mitigate and protect against the resulting threats." Before continuing and highlighting the multiple challenges that this phenomenon poses: "these threats, which weigh in particular on the stability cyber, human rights, national security and digital security as a whole are expected to intensify in the years to come."

In its 2023 Threat Overview, also published in February 2024, the National Information Systems Security Agency (ANSSI) confirms the observation: "if these capabilities are historically developed by States possessing advanced offensive capabilities, the growth of the private surveillance

market is confirmed: certain companies provide very sophisticated malicious codes to public actors, but also to companies and individuals with malicious intentions. The proliferation of commercial offensive tools contributes significantly to the overall increase in threat levels."

The massive emergence of commercial intrusion capabilities is likely to lead to a transformation of state practices. On an international scale, we are already very clearly observing excesses in the use of these capacities, which is regularly the subject of various publications; it is therefore appropriate to define a framework for responsible use.

The necessary definition of a framework for responsible use: the French model

The cyber intrusion industry meets diverse needs and the products that result from it often have a dual nature. They can thus be used for cybersecurity purposes (intrusion test to check the robustness of a computer system for example), for national security purposes, but they can also be misused. For example, data capture software which would play a vital role in an anti-terrorist investigation or in the fight against organized crime can also be used for the purposes of surveillance of political opponents and journalists in conditions contrary to the law. respect for the rule of law. From this complexity arises the need to avoid any simplistic approach, such as prohibition, to focus on the notion of responsible use and associated control mechanisms. This is why the Pall Mall Process has made it – along with the question of shaping the market itself – one of its areas of work.

Regarding usage control mechanisms, the Pall Mall Process approach is intended to be empirical and is intended to begin with a benchmarking of current practices. France, where the major balances of intelligence law are exclusively defined by the national legislator, under the control of the Constitutional Council, can promote its model which subordinates the use of capabilities detrimental to private life to the authorization of a magistrate. for judicial investigations, and the obligatory and prior

obtaining of the opinion of an independent administrative authority for administrative investigations. In this context, the CNCTR carries out a control of the legality and proportionality of the request. If his opinion is not followed by the Government – which has never happened until now – the supreme administrative judge (Council of State) is immediately referred.

Among the other means available to States to control the proliferation and use of cyber-intrusion capabilities, export control is often cited. In fact, intrusion software has been covered since 2013 by the Wassenaar Arrangement, a multilateral export control regime for conventional weapons and dual-use goods and technologies of which France is a part. Less well known are the import control mechanisms, to which, for example, the "R. 226" system in France, named after the article of the French Criminal Code which constitutes its legal basis[58], contributes. This interministerial system within which the CNCTR sits makes it possible to exercise control over imported materials likely to compromise the secrecy of correspondence, including data capture software for example.

A multi-actor effort towards better regulation

While a follow-up conference of the Pall Mall Process will be organised in France in 2025, the next stages of the initiative are gradually taking shape. Among them, the desire to exchange between stakeholders on best practices on the part of States, companies or even civil society to help fight against the proliferation and irresponsible use of cyber intrusion capabilities available on the walk.

Ultimately, the ambition of this "soft law" type process is to create a body of rules of good conduct, similar to those governing the activities of security and defence services companies (ESSD), also called the Montreux Document, adopted in 2008. There is no doubt that the question of control will be a key element of this international regulation effort.

58. "The manufacture, import, exhibition, supply, rental or sale of any device or technical equipment appearing on the list mentioned in Article R. 226-1 is subject to authorisation issued by the Prime Minister, based on the opinion issues by the Commission mentioned in Article R. 226-2. "

Appendices

1. Change in the make-up of the CNCTR's committee over the course of 2023

The composition of the CNCTR college saw a renewal concerning one of its members in 2023.

On 6 November 2023, Mr Jérôme DARRAS, senator from Pas-de-Calais, was appointed member of the CNCTR by the President of the Senate. He succeeded Mr. Yannick VAUGRENARD, whose mandate had come to an end.

At the end of 2023, the CNCTR college was made up of following nine members:

- **Mr Serge LASVIGNES**, Honorary State Councillor, Chairman
- **Ms Chantal DESEYNE**, senator of Eure-et-Loir;
- **Mr Jérôme DARRAS**, senator of Loire-Atlantique;
- **Ms Michèle TABAROT**, member of Parliament for Alpes-Maritimes (Assemblée nationale);
- **Mr Yannick CHENEVARD**, member of Parliament for Var (Assemblée nationale);
- **Ms Françoise SICHLER-GHESTIN**, Honorary State Councillor;
- **Ms Solange MORACCHINI**, honorary general advocate at the Court of Cassation;
- **Mr Gérard POIROTTE**, honorary advisor to the Court of Cassation;
- **Mr Philippe DISTLER**, qualified personality in electronic communications.

The terms of designation or appointment of members are set by Article L. 831-1 of the French Internal Security Code With the exception of parliamentary members, their mandate 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. Furthermore, with the exception of the qualified personality, the law provides that the methods of designation or appointment of members of the commission ensure equal representation of men and women.

Under the provisions of Article L. 831-2 of the French Internal Security Code, the plenary body of the Commission includes all its members and the restricted body is made up of all members who are not members of parliament.

2. The CNCTR's resources

2.1. Human resources

Since 1 November 2023, of the 9 members of the Commission's college, four are now full-time members. These are the chairman of the CNCTR, the two honorary members of the Court of Cassation and the qualified personality.

This reinforcement of the daily presence of members having the status of magistrate[1] was made necessary by the intensification of the ex-post control activity of the Commission[2] as well as by the increase in the number of technical requests submitted to it. The provisions of the French Internal Security Code impose a period of twenty-four hours on the CNCTR to give its opinions on requests for which examination in college is not required; these opinions can only be given by members having the status of magistrate.

When the request submitted to the commission falls under the plenary body or the restricted body, or when it is referred to such a body, the time limit is extended to seventy-two hours[3]. Consequently, these bodies meet, except in exceptional cases, three times a week, Mondays, Wednesdays and Fridays, all year round, which represents more than 140 sessions per year, to which is added each month a solemn meeting of the whole of its members in a plenary formation. These plenary meetings monthly meetings usually begin with a hearing (National Intelligence and Counter-Terrorism Coordinator, department heads, director of the Inter-Ministerial Control Group, chief of staff of the ministers responsible for the services, etc.), give rise to the examination of the most important draft deliberations and also include time devoted to the activity of the commission, whether on substantive subjects or statistical elements.

1. Members referred to in Article L. 831-1 (2) and (3) of the French Internal Security Code
2. See point 2.1.1 in this report.
3. See the provisions of Article L. 821-3 of the French Internal Security Code.

In parallel with these collegial training courses, frequent meetings, presentations and hearings are organized in the commission's premises in order to enlighten the college on technical or legal subjects.

For its operation, the CNCTR's body relies on a team comprising, as of 31 December 2023, 20 agents: a general secretary, an advisor placed under the chairman, 14 project managers[4]4 and 4 agents assigned to support functions (one responsible for budgetary and human resources issues responsible for supervising the secretarial division, two executive assistants and a driver also responsible for the duties of assistant security officer).

The CNCTR's mission managers are, essentially, category A+ and similar agents, whose main role is to examine requests for the implementation of intelligence-gathering techniques and to conduct ex-post controls, under the supervision of a member of the commission.

They are, more or less equally, either seconded public agents (judicial and administrative magistrates, police commissioner, armaments engineer) or contract agents (notably engineers). Added to this is a senior gendarmerie officer made available to the CNCTR against reimbursement of his remuneration. Given the instruction and control missions entrusted to them, the agents of the commission are mainly recruited for their legal or technical skills.

The secretariat staff is made up of two permanent civil servants and two contract agents.

The CNCTR team is made up of 55% women and 45% men. The average age of agents is 39 years old.

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

4. Including a technical advisor and a coordinator of ex-post control activities.

2.2. The budget

The credits allocated by Parliament to the CNCTR are included in the general State budget ("Direction of Government Action" mission, program no. 308 "Protection of rights and freedoms", action no. 12 "National Oversight Commission for Intelligence-Gathering Techniques").

The initial finance law for 2023[5] allocated to the CNCTR amounts of just over 2.7 million euros for its personnel expenses (T2) and a little over 400,000 euros for its operating expenses.

In accordance with the creation of positions which were granted to the commission for the years 2022, 2023 and 2024[6], it was possible to carry out two recruitments in 2023 (two project managers with a generalist profile) as well as the turning into a full-time position of the position of a member of the college. Strengthening the technical centre is more complicated to achieve. Two recruitments are therefore still planned for 2024.

The context, described in the body of the activity report, the increase in the number of requests for techniques, the need to guarantee the efficiency of the ex-post control capacity both from a quantitative and qualitative point of view, finally the increase in the number of complaints, mean that the continuation of this upward trend in both the staff and the operating budget of the commission appears essential to the successful accomplishment of the missions entrusted to it by the law-maker. Beyond that, in the medium term, the question of resizing the commission will arise so as to reach a critical size allowing it to secure the various support functions.

5. 2023 Budget law No. 2022-1726 of 30 December 2022

6. See the 7th 2022 CNCTR activity report, p. 64 and following and p. 134.

3. The CNCTR's external relations

In 2023, the Commission continued its fruitful dialogue with its institutional partners, the academic world but also its foreign counterparts. She also provided a certain number of training courses for the benefit of various public entities. These numerous exchanges and interactions allow the commission to share its point of view on the legal framework applicable to intelligence and, where applicable, to raise its expectations in this area. They also help to disseminate knowledge of this legal framework, improve practices and benefit from the experience of the commission's foreign counterparts in this area.

3.1. A conference co-organized with the DPR

In May 2023, the CNCTR co-organised with the Parliamentary Delegation for Intelligence (DPR), a **conference devoted to the control of public intelligence policy**. Opened by the chairman of the National

Assembly, this conference, which was held at the Hôtel de Lassay, brought together members of Parliament, magistrates, representatives of the intelligence services and independent administrative authorities, as well as academics. It was an opportunity to debate the modalities for effective mobilization of intelligence in a world heavier with threats, while ensuring effective protection of freedoms and private life in the face of the strengthening of the services' resources and the rapid development of surveillance technologies.

3.2. A dialogue maintained with Parliament

Concerning more particularly the **institutional dialogue maintained with Parliament**, the chairman of the CNCTR was heard five times by the Senate in 2023:

- in May, he was heard by Mr Philippe Bas, rapporteur of the **draft law relating to biometric recognition in public spaces**[7] for the Law Commission. He was notably questioned about the possibilities of using artificial intelligence technologies to facilitate the processing of data collected as part of intelligence-gathering techniques or to make the results of analyses carried out by the services more reliable, as well as the methods of supervision of a possible experiment with biometric recognition in public spaces;

- in June, he was heard by Mr Christian Cambon, rapporteur for the Committee on Foreign Affairs, Defence and Armed Forces, on the **military programming bill for the years 2024 to 2030** which led to law No. 2023-703 of 1 August 2023;

- in July, he was received by the **information mission on the methods of investigation using connection data in within the framework**

7. Refer to the legislative file on the Senate's website: *https://www.senat.fr/dossier-legislatif/ppl22-505.html*.

of criminal investigations[8], and questioned on the operation of the special legal regime governing access to this data in matters of administrative policing, as well as on the modifications made by Law no. 2021-998 of 30 July 2021 relating to prevention acts of terrorism and intelligence to bring French legislation relating to intelligence into compliance with European Union law governing the retention by electronic communications operators of their subscribers' data;

- and in October 2023, he was interviewed by the rapporteur for the Laws Committee in the budget opinion procedure relating to the "Direction of government action" mission during the examination in the Senate of the draft law finances for 2024.

Furthermore, it was heard twice in the National Assembly:

- in July, he was questioned by the rapporteurs of the **fact-finding mission on generative artificial intelligence**[9] and shared his thoughts on the perspectives opened up by the development of artificial intelligence in terms of intelligence, and its possible consequences for the control activity of the commission, emphasizing the importance of close human supervision, as the tools concerned improve and their areas of application diversify[10];

- also in July, he was interviewed by the **commission of inquiry into the structuring, financing, means and methods of action of small groups responsible for violence during the demonstrations and gatherings which took place between 16 March and 3 May 2023 as well as on the progress of these demonstrations and gatherings**[11]. In particular, it was heard about the sufficiently exhaustive nature of the current legal framework with regard to the prevention of collective violence.

8. See: https://www.senat.fr/notice-rapport/2023/r23-110-notice.html.

9. See:https://www.assemblee-nationale.fr/dyn/16/organes/commissions-permanentes/lois/missions-d-information-de-la-commission-des- lois/intelligence-artificielle-protection-donnees-personnelles.

10. Also refer to the above "Insights" section of this report about this topic.

11. See: https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cegrvimani/l16cegrvimani2223021_compte-rendu#

3.3. The other institutional points of contact of the Commission

The chairman of the CNCTR was also interviewed in January 2023 by the members of the **European Parliament committee specially responsible for investigating the use by certain States of the surveillance software known as "Pegasus"**[12], in order to inform them of the legal framework governing the use of intelligence-gathering techniques in France. He described its founding principles and testified to the way in which it works, reporting in particular the limits it imposes on the intelligence services as well as the original characteristics of the system provided in France for the control of their action. He also formulated avenues for reflection for the supervision of this type of surveillance tools by the national legislator.

The commission was also heard three times by the Court of Auditors as part of its mission of auditing the accounts and management of the intelligence services.

3.4. The international relations of the commission

Regarding international relations, the CNCTR continued to maintain a dialogue with its foreign counterparts within the framework of bilateral but also multilateral meetings.

A delegation from the commission thus participated on 9 and 10 November 2023, in Oslo, at the **European Intelligence Control Conference**, which brings together each year national control authorities from many European countries.

The discussions focused in particular on the use of public data, the methods of effective control, the case law of the European Court

12. See: *https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/OJ/2023/01-09/1269403FR.pdf*.

of Human Rights as well as the responsibility of control bodies and the methods of publicizing their activity.

Finally, at the end of November 2023, the CNCTR contributed to the sixth edition of the **International Intelligence Oversight Forum** which took place this year in Washington DC and which notably addressed the question of the need and the proportionality of surveillance.

3.5. Training to which the commission contributed

Over the past year, the commission also continued its participation in the training effort for agents of the intelligence services as well as executives of their supervisory ministries to develop within them knowledge of the legal framework applicable to surveillance techniques. information. The Commission thus intervened almost ten times in 2023 before the auditors of the **Intelligence Academy**.

In addition, she contributed to two training sessions provided by the National School of Magistrates and spoke twice at the **Center for Advanced Military Studies** (CHEM).

3.6. Communication towards the general public

Finally, more generally and aimed at the general public, in addition to the publication of its annual activity report, the CNCTR continued its effort to make available information as detailed as national defence secrecy allows on its mission and exercise of its control action.

In this regard, as a continuation of the overhaul of its website[13] which took place in 2023, the Commission has enriched the resources accessible there, in particular with numerous thematic fact sheets on the purposes enabling the use of intelligence-gathering techniques provided for by the French Internal Security Code, the content of these techniques and their scope.

13. *https://www.cnctr.fr/*

4. Ruling No. 2/2023 of 16 November 2023 on the adoption of the rules and regulations of the National Oversight Commission for Intelligence-Gathering Techniques

Article 1

The new rules and regulations of the National Oversight Commission for Intelligence-Gathering Techniques, in the version appearing in the appendix, are adopted.

Article 2

Deliberation No. 2/2017 of 23 March 2017 adopting the rules and regulations is repealed.

Article 3

The Secretary General of the National Oversight Commission for Intelligence-Gathering Techniques is responsible for the execution of this decision which will be published in the Official Journal of the French Republic.

Appendix

Rules and regulations of the National Oversight Commission for Intelligence-Gathering Techniques adopted by the Commission meeting in plenary session on 16 November 2023.

Title 1 – Ethical rules applicable to the members and agents of the National Oversight Commission for Intelligence-Gathering Techniques

Article 1 – Independence

The members and the agents of the National Oversight Commission for Intelligence-Gathering Techniques, hereafter referred to as "the Commission", refrain from any behaviour likely to raise doubts about the institution's independence.

They abide by a general obligation of loyalty to the institution.

They neither request nor receive instructions from any authority.

Article 2 - Preventing conflicts of interests

I. - When the members and the agents of the Commission consider that their taking part in a deliberation or a control could be regarded as a potential situation of conflicts of interest, or for any other reason whatsoever, on their own initiative or that of someone else, their independence is not or may not look assured, they undertake to inform the Chairman as soon as they are aware of the situation, and at the start of the involved deliberation or control, at the latest. They refrain from taking part in the involved deliberation or control and from issuing an opinion. The Chairman shall inform the other members of the Commission without delay of the conflicts of interest he/she is aware of as per the previous paragraph or those involving him/her.

II. - The members and the secretary general send to the chairman of the Commission a copy of the declaration of interests provided for in 6° of Article 11 of Law no. 2013-907 of 11 October 2013 relating to the transparency of public life. The declaration of interests of each member is made permanently available to other members in the premises of the commission. The chairman returns to the members and the general secretary their declaration of interests within six months following the end of their functions within the commission.

Article 3 – National defence secrecy, professional confidentiality, professional discretion

The members and agents of the Commission observe national defence secrecy under the conditions provided for by General Interministerial Instruction No. 1300 on the protection of national defence secrecy as well as professional confidentiality and the duty of professional discretion to which they are required by law.

These obligations continue after the end of the mandate of member or agent of the Commission.

National defence secrecy cannot be enforced between members and agents of the commission. They owe each other all the information useful to the successful accomplishment of their missions.

Sharing national defence secrecy with a service or agent outside the commission for the processing of a file does not authorize disregard of the secrecy covering another matter.

No particular or general matter covered by national defence secrecy may be discussed with a service or agent who does not need to know about it or is not authorized to do so.

Article 4 – Fair-mindedness

Requests submitted for opinion to the commission are examined impartially and neutrally.

Entrusted with a mission of controlling the services authorized to implement intelligence-gathering techniques, the members and agents of the Commission can only have relations with the agents of these services that are compatible with the exercise of such control.

Article 5 – Behaviour when conducting checks

During checks, members and agents of the commission submit to the security rules applicable in the intelligence services concerned.

They never deviate from the required courtesy.

They ask those in charge of the premises as well as the operating agents to allow them access to the data that is useful to them and to provide them with the documents necessary to carry out the inspection. They precisely record any refusal to access data, whether accidental or deliberate, and, more generally, any refusal to cooperate which could compromise the conduct of their mission.

They refrain from any judgment during the visit. They limit themselves to collecting the information that is useful to them, establishing its veracity and asking the questions required for their understanding.

They ensure that the questions they ask are directly related to the responsibilities of the commission. They specify as necessary how their requests fall within these responsibilities.

In their report, they take complete objective care to distinguish between established facts and hypotheses and highlight the considerations which appear to them to merit examination by the members of the commission.

Article 6

Any difficulty encountered by the members and agents of the commission in the exercise of their missions is brought to the attention of the chairman, who can invite the restricted or plenary formation of the commission to debate.

Article 7 – Suspension of terms of office, end of functions or resignation of a member

The plenary body of the commission deliberates over the suspension of the term of office, the end of the functions or the resignation of a member for one of the reasons provided for in Article 6 of Law No. 2017-55 of 20 January 2017 pertaining to the general status of independent administrative authorities and independent public authorities.

The deliberation takes place at least one week after the interested party has been able to provide written observations or, at his/her request, to be heard by the plenary panel. The vote takes place by secret ballot without the person concerned being present.

Article 8 – Pledge

When they take up their duties, the members and agents of the commission pledge that they undertake to respect the provisions of these rules and regulations.

Title II - Organization and functioning of the commission

Chapter I - Plenary and restricted training

Article 9 – Calendar of plenary and restricted training sessions and agenda

The plenary and restricted formations set the schedule of their meetings. They are also brought together as necessary, at the initiative of the chairman.

In the case provided for in Article L. 821-7 of the French Internal Security Code, the chairman takes the necessary measures to convene the plenary session as soon as possible.

The chairman sets the agenda for the plenary and restricted meetings of the commission. Commission members may request the inclusion of a question on this agenda.

Useful documents are made available to members in the commission's premises no later than twenty-four hours before the meeting.

By way of derogation from the previous paragraph, when the commission is requested to render an opinion on a request for the implementation of one of the intelligence collection techniques mentioned in Chapters I to IV of Title V of Book VIII of the French Internal Security Code, useful documents are made available to members of the commission as soon as possible.

Article 10 – Presidency of the plenary and restricted bodies

The plenary and restricted formations of the commission are chaired by its chairman who directs the debates.

In the event of the absence, incapacity or removal of the president, or if the position of chairman becomes vacant for any reason whatsoever, the presidency of the plenary and restricted formations is ensured

by the most senior member of the Commission among the members mentioned in 2° and 3° of Article L. 831-1 of the French Internal Security Code. In the event of competition in seniority between several of these members, the presidency is exercised by the oldest member among them.

Article 11 – Opinions and deliberations of the Commission

I. - The plenary and restricted bodies of the Commission decide by a majority of the members present or participating in the deliberation, the chairman having the casting vote in the event of an equal division of votes. As necessary, the chairman may decide to use the means of remote deliberation provided for by Ordinance No. 2014-1329 of 6 November 2014 relating to remote deliberations by collegial administrative bodies, as long as the identification of participants, the confidentiality of the debates and the protection of national defence secrets are ensured.
Unless the chairman decides otherwise, the secretary general and the agents of the commission attend the plenary and restricted sessions.

II. - The secretary general of the commission or, in the event of his absence or incapacity, the agent of the commission designated by the chairman, provides secretarial services for the sessions of the plenary and restricted formations and draws up the minutes.
When the commission is requested to render an opinion on a request for the implementation of one of the intelligence collection techniques mentioned in Chapters I to IV of Title V of Book VIII of the French Internal Security Code, the indication of the panel having examined the request, the members present and the meaning of the decision rendered, recorded on the request instruction sheet, may serve as minutes. The minutes, opinions and deliberations of the Commission, as well as the follow-up given to these opinions by the Prime Minister, are made available to members in the Commission's premises.

Article 12 – Doctrine

The plenary or restricted body discusses the principles governing the opinions issued by the Commission on the requests submitted to it as well as its controls carried out on the implementation of intelligence-gathering techniques.

Article 13 – Controls

In consultation with the members of the Commission, the chairman decides on the program of control visits and the conditions under which these visits are organised. He/she can also decide on impromptu checks.

Checks can also be carried out remotely.

The results of the controls and the action taken by the services concerned are brought to the attention of the plenary or restricted bodies of the Commission.

Article 14 – Follow-up to the opinions of the Commission

I. – When the authorisation mentioned in Article L. 821-1 of the French Internal Security Code is issued by the Prime Minister after a negative opinion issued by the Commission, the chairman of the Commission or, failing that, one of the members of the Commission, mentioned in 2° and 3° of Article L. 831-1 of the said code, immediately refers the matter to the Council of State and informs the plenary session as soon as possible.

II. - The plenary session is informed of the recommendations addressed to the Prime Minister, tending that the implementation of a technique be interrupted and the information collected destroyed, in application of Articles L. 833-6 or L. 854-9 of the French Internal Security Code. It debates the follow-up given by the Prime Minister to these recommendations.

III. - The plenary session decides on the observations it deems useful to send to the Prime Minister in application of Article L. 833-10 of the French Internal Security Code.

Article 15 – Requests for opinions pursuant to Article L. 833-11 of the French Internal Security Code

The plenary session debates the response that shall be given to requests for advice that the Prime Minister, the President of the National Assembly, the President of the Senate and the parliamentary intelligence delegation, as per the provisions of Article L. 833- 11 of the French Internal Security.

Chapter II - Organization of the commission and processing of requests

Article 16

The agents of the Commission are placed under the authority of the Chairman. They assist the members of the commission in carrying out their missions.

The general secretary leads and coordinates their action.

Article 17

The chairman sets, in consultation with the members and agents of the commission, the conditions under which opinions are rendered on requests for the implementation of intelligence gathering techniques mentioned in Chapters I to IV of Title V of Book VIII of the French Internal Security Code subject to it.

The chairman ensures that the deadlines given to the commission to issue its opinions are respected.

Article 18

All requests submitted to the commission are examined in light of the information communicated, which is interpreted strictly, without alteration or omission.

When all the information necessary to examine the request has not been communicated, the commission invites the service originating the request to send it additional information as soon as possible.

The legal examination period runs from the moment the commission considers that the application is complete.

Article 19

Any new question or any serious difficulty is, at the initiative of the chairman or one of the members of the commission, submitted, as the case may be, to the plenary or restricted formation of the commission.

Chapter III - Public reporting, communication and external relations

Article 20

In its institutional relations, the commission is represented by the chairman who reports to the plenary session.

The public communication of the commission is ensured by the chairman, in consultation with the members.

The agents of the commission cannot speak on behalf of the institution, unless expressly mandated by the chairman.

Article 21

The public activity report, debated and approved in plenary session, is submitted by the chairman to the President of the Republic, the Prime Minister and the presidents of the two assemblies.

The chairman invites the parliamentarians who are members of the commission to accompany him during his visit to the president of the assembly in which they sit.

Article 22

The chairman, in consultation with the members and agents of the Commission, takes all measures to conduct useful exchanges in the European and international frameworks and promote the French model of control of intelligence-gathering techniques.

Photo credit: Damien Carles / Matignon, Assemblée nationale, Sénat.

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

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

Maquette (numérique) : DSAF / DPSG / BAEC / Section Édition – 26 juillet 2024 - ISSN XXXX-XXXX