CNCTR

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

# 9e Rapport d'activité 2024

À Serge LASVIGNES (1954-2025)

Président de la CNCTR d'octobre 2021 à janvier 2025

# Avant-propos

Le rapport d'activité de la Commission nationale de contrôle des techniques de renseignement est prévu par la loi. Rendu public, il est destiné au public. Depuis l'origine, il expose, sans enfreindre le secret de la défense nationale, l'accomplissement de ses missions par la commission. Plus essentiellement, il cherche à rendre compte du respect, dans l'emploi des techniques de renseignement, de l'équilibre voulu par la loi entre le respect de la vie privée, d'une part, et la défense et la promotion des intérêts fondamentaux de la Nation, d'autre part.

Président de la CNCTR d'octobre 2021 au 31 janvier 2025, Serge Lasvignes a particulièrement veillé à cet équilibre comme à la manière d'en faire rapport. Il a mis en lumière les lignes de force qui en attestent aussi bien que les risques qui peuvent l'atteindre ou que les incertitudes juridiques et techniques qui le fragilisent. Il a prolongé le récit de chaque année d'activité par des études thématiques, offrant compréhension et perspectives.

Serge Lasvignes a assumé sa fonction jusqu'à ce que la maladie le contraigne à s'en retirer. Il est décédé le 15 février 2025. Les membres du collège et les collaboratrices et collaborateurs de la CNCTR saluent avec attachement et respect sa mémoire et lui dédient ce rapport d'activité.

**2024 : une activité maîtrisée dans une année particulière**

Le constat le plus marquant au sujet de l'année 2024 est qu'elle n'a pas été l'occasion d'une explosion du recours aux techniques de renseignement, malgré le caractère exceptionnel des événements, prévus ou imprévus, qui l'ont jalonnée : élections européennes puis législatives, parcours de la flamme olympique puis Jeux olympiques et paralympiques de Paris 2024, réouverture de la cathédrale Notre-Dame de Paris, émeutes et état d'urgence en Nouvelle-Calédonie, troubles violents en Martinique et en Guadeloupe.

En effet, dans ce contexte, le nombre de demandes d'emploi de techniques de renseignement examinées par la commission n'est passé que d'un peu moins de 95 000 en 2023 à un peu moins de 99 000 en 2024 et le nombre de personnes surveillées est demeuré constant : 24 209 en 2023 puis 24 308 en 2024, selon les estimations de la commission. La part des avis défavorables rendus par la commission est presque identique : 1,2% en 2023, 1,3% en 2024. Si le contingent des « écoutes téléphoniques » a été momentanément augmenté, ce fut dans la limite préconisée par la CNCTR.

On pourra retenir de ces constats que les services de renseignement, sous l'autorité des pouvoirs publics, l'égide de la Coordination nationale du renseignement et de la lutte contre le terrorisme et le contrôle de la CNCTR, ont gardé la maîtrise de la situation et conservé le cap d'une action mesurée et sélective.

La chronique particulière de 2024 laisse toutefois son empreinte dans les finalités vers lesquelles est dirigé le renseignement. La prévention du terrorisme redevient, en 2024, le premier motif de surveillance en nombre de personnes concernées, après qu'en 2023 et pour la première fois, il se fût agi de la lutte contre la criminalité organisée.

La CNCTR n'a pas manqué d'adapter son action à cette année hors norme. Si le nombre des contrôles effectués dans les services n'a que très légèrement reculé : 123 en 2024, après 136 en 2023, la période des Jeux a été évitée autant que faire se pouvait et davantage de contrôles ont été faits à distance. Pour autant, les échanges thématiques avec les services de renseignement, à leur initiative ou à la demande de la commission, n'ont reculé ni en nombre ni en qualité. La commission y voit un élément essentiel de sa relation avec ces services. Ils permettent tantôt de comprendre en profondeur une menace ou un phénomène vers lesquels s'oriente l'action des services, tantôt d'améliorer la vision de la commission, par-delà le caractère nécessairement ponctuel des contrôles, souvent de rechercher les voies d'une amélioration technique ou d'une évolution doctrinale souhaitables.

### Des anomalies persistantes dix ans après la loi sur le renseignement

Les relations confiantes que la CNCTR entretient avec les services de renseignement ne la dispensent pas de relever une nouvelle fois la persistance d'anomalies. Les plus sérieuses d'entre-elles concernent l'exploitation des données recueillies, dans des « bulletins de renseignement ». Ils sont essentiels pour apprécier l'utilité et la justification légale de la mesure de surveillance après son autorisation. Leur examen permet aussi de vérifier que les informations conservées après l'effacement des données brutes au terme du délai légal sont bien en lien avec la finalité poursuivie. Or, on ne les trouve pas toujours là et quand on devrait les trouver. De même, la conservation imparfaite des traces exactes des opérations conduites ou, plus rarement, le dépassement de la durée de validité d'une autorisation de mettre en œuvre une technique de renseignement ou encore la méconnaissance de limites posées par la commission dans l'avis qu'elle a rendu sur la demande d'un service font encore partie des anomalies constatées par la commission.

La CNCTR exprime à nouveau sa confiance dans les services de renseignement et dans leur légalisme. Elle est consciente, aussi, des difficultés qu'ils rencontrent, des priorités opérationnelles qui s'imposent à eux tout comme des efforts nécessaires pour assurer partout et de façon homogène le respect du cadre légal. Dès lors, elle les invite à mettre en œuvre des plans d'action précis, partagés et suivis afin de garantir efficacement et durablement que la loi soit bien appliquée par tous et que la commission, par son contrôle, par le dialogue avec eux ou par la construction de sa doctrine puisse y veiller pleinement.

### Des évolutions attendues

Aux mêmes fins, la CNCTR place de grandes attentes dans la mise en œuvre de l'orientation décidée à la fin de l'année 2023 par le Président de la République de centraliser au Groupement interministériel de contrôle (GIC) l'ensemble du produit des recueils

de données informatiques (RDI). Cette technique, qui prend des formes variées, est particulièrement intrusive. Or, elle est à la fois employée de façon croissante et difficile à contrôler lorsque ses traces sont disséminées dans les services.

La commission souligne que la centralisation doit, à parts égales, lui permettre un contrôle effectif du RDI et offrir aux agents des services de renseignement un outil de travail unifié et plus accessible, tout en renforçant la fonction du GIC.

Comme convenu, les études techniques ont commencé, sous le pilotage de la Coordination nationale du renseignement et de la lutte contre le terrorisme, à l'automne 2024, une fois passés les Jeux de Paris. Pour que le dispositif soit en place mi-2027, ainsi qu'il a été décidé, des ressources importantes et des efforts soutenus sont indispensables. La commission y porte une très grande attention ; les années 2025 et 2026 seront décisives.

### Une année d'initiative parlementaire

Sur le plan législatif et parlementaire, l'année 2024 a été marquée en premier lieu par la loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France[1]. Elle a vu, en second lieu, la publication du rapport d'une commission d'enquête du Sénat sur l'impact du narcotrafic en France[2] puis, le dépôt d'une proposition de loi sur le même thème[3].

Un point commun de ces deux textes est de prévoir l'extension de la technique de renseignement dite de l'algorithme, introduite dans le code de la sécurité intérieure par la loi de 2015 aux fins de la lutte contre le terrorisme, à la détection respectivement des

1. Voir loi n° 2024-850 du 25 juillet 2025 visant à prévenir les ingérences étrangères en France.
2. Sénat, 7 mai 2024, rapport n°588 fait au nom de la commission d'enquête sur l'impact du narcotrafic en France et les mesures à prendre pour y remédier ; président : M. Jérôme Durain, rapporteur : M. Étienne Blanc.
3. Sénat, 12 juillet 2024, proposition de loi n°735 rect. visant à sortir la France du piège du narcotrafic, présentée par MM. Étienne Blanc et Jérôme Durain, sénateurs.

ingérences étrangères et du narcotrafic. Dans les deux cas, le Parlement a trouvé dans la montée des menaces la justification légitime de l'emploi de cette technique particulière.

Le présent rapport saisit cette occasion pour exposer dans une étude dédiée le cadre juridique de l'algorithme. Il importe, en effet, de dissiper les craintes que suscite le terme même d'algorithme. Ce que permet le code de la sécurité intérieure n'est ni une surveillance de masse ni un automatisme. L'exercice de contrôle de la CNCTR à chaque étape, en particulier pour autoriser un projet d'algorithme, puis pour rendre des avis sur chaque levée de l'anonymat après d'éventuelles détections issues du traitement algorithmique et enfin sur la demande de mise en œuvre de techniques de renseignement à l'encontre des personnes concernées, protège du risque de surveillance de masse. L'examen par le service puis par la commission du bien-fondé de chaque détection et des conséquences à en tirer préserve le principe de primauté humaine[4] et préserve du risque d'automatisation pure et simple.

**Une décision importante de la CEDH et des questions encore en suspens**

Sur le plan jurisprudentiel, 2024 a vu la Cour européenne des droits de l'homme délibérer sur une décision longtemps attendue, puisqu'elle statue sur des requêtes présentées en 2015 et en 2017[5].

Au terme d'un examen très détaillé, la décision de la CEDH reconnaît que le cadre légal français garantit à toute personne un droit à un recours effectif contre l'emploi à son encontre de techniques de renseignement. La Cour se prononce, en particulier, sur l'indépendance de la CNCTR et l'effectivité de son contrôle ainsi que sur la bonne articulation des procédures de réclamation

4. Voir notamment : Conseil d'Etat, étude à la demande du gouvernement, « intelligence artificielle et action publique : construire la confiance, servir la performance », 31 août 2022.

5. Voir partie 3.1 du rapport d'activité.

préalable devant elle puis de recours devant le Conseil d'Etat siégeant en formation spécialisée.

Il est permis de voir dans cette décision la confirmation que la loi et la pratique françaises donnent à la politique publique du renseignement un cadre équilibré, respectueux des libertés comme de la défense et de la promotion des intérêts fondamentaux de la Nation. C'est, par ailleurs, ce qu'avaient, cette même année 2024, permis de débattre et de constater deux utiles colloques co-organisés par la CNCTR[6].

Le paysage juridique et opérationnel du renseignement n'est pas pour autant exempt de lacunes ou de fragilités. Par exemple, il convient de souligner ici une nouvelle fois que la France ne connaît pas d'encadrement légal des échanges d'information entre services nationaux et étrangers. Ceci est, de manière certaine, contraire à la jurisprudence internationale[7]. Dans un monde de menace globale, de tels échanges sont légitimes et indispensables. Leur donner un statut légal ne l'est pas moins ; les droits et libertés ne peuvent pas être garantis sur un flanc seulement.

## Dix ans et des perspectives

L'année 2025 est celle du dixième anniversaire de la loi du 24 juillet 2015 relative au renseignement, qui a écrit le livre VIII du code de la sécurité intérieure et institué la commission nationale de contrôle des techniques de renseignement. C'est donc aussi l'anniversaire de la mise en place de la commission, à la suite de la commission nationale de contrôle des interceptions de sécurité.

Ces dix années ont tout à la fois mis notre pays à l'épreuve d'attaques et de risques graves et confirmé l'efficacité d'un cadre légal qu'il n'a été nécessaire de modifier qu'à la marge.

6. Conférence internationale co-organisée par la CNCTR et la revue Etudes françaises de renseignement et de cyber : « *les enjeux du contrôle du renseignement : un dialogue des contrôleurs ?* », Paris, 15 octobre 2024 – Commission nationale informatique et libertés, « avenirs, innovations, révolutions 2024 » : « *la surveillance dans tous ses états : quelle éthique pour (protéger) nos libertés* », Paris, 19 novembre 2024.

7. v. notamment : CEDH 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, req. N°s 58170/13, 62322/14 et 24960/15.

Pour la commission, qui pense avoir elle aussi rempli sa mission, l'occasion est moins celle de l'autocélébration que celle de la réflexion, en lien avec la communauté française du renseignement, les représentants parlementaires et tous ceux qui montrent leur intérêt au débat.

Deux axes au moins méritent réflexion. Le premier est celui du principe légal de proportionnalité. Il est mis à l'épreuve de la technique, dès lors que le recours aux techniques de renseignement les plus intrusives survient plus tôt et augmente en général. Le principe s'applique aussi à la durée de la surveillance, qui peut poser question lorsqu'elle n'est renouvelée que dans l'attente d'éléments décisifs. Le propre de la police administrative en matière de renseignement est de rechercher pour prévenir. L'action publique se conduit donc sous l'aléa de l'hypothèse et au risque de l'incertitude. Toutefois, dans la dimension technique comme dans la dimension chronologique, il ne faut ni subir ni s'accoutumer.

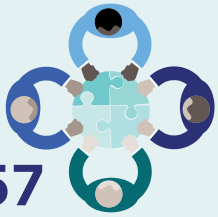
Le second axe est celui de la coopération entre la commission et les services de renseignement des deux cercles. C'est un acquis solide de dix années ; il faut le cultiver. La commission y invite les services de renseignement à toutes les étapes : motivation des demandes de techniques de renseignement, pour en garantir la bonne appréciation, disponibilité lors des contrôles *a posteriori*, pour en assurer l'utilité et permettre des suites effectives, échanges thématiques, afin de surmonter la dissymétrie des savoirs techniques, de comprendre les risques qu'il incombe aux services de prévenir et d'identifier les points de doctrine qui demandent clarification ou évolution. Garante de droits intangibles comme de l'action légale des services de renseignement, chargés de protéger contre des menaces changeantes et souvent croissantes, la CNCTR renouvelle ici son engagement.

**Vincent Mazauric**
Conseiller d'Etat
Président de la CNCTR

# Les chiffres clés

**98 883**
demandes de techniques de renseignement
(techniques domestiques individuelles)*

**24 308**
personnes surveillées



**157**
réunions collégiales

**123**
contrôles
dans les services de renseignement

**3,4 millions €**
de budget

*Cette donnée n'inclue pas les demandes non-individualisées et/ou relevant des mesures de surveillance des communications électroniques internationales ce qui recouvre les demandes ayant trait à la technique dite de l'algorithme prévue à l'article L. 851-3 du code de la sécurité intérieure, les demandes de transmissions de renseignement subordonnées à un avis préalable de la commission mentionnées au II de l'article L. 822-3 du même code ou les autorisations d'exploitation mentionnées à son article L. 854-2 (voir respectivement p. 42 et p. 49 ci-dessous).

# de l'année 2024

**10 déplacements**
dans les territoires
dont **1 outre-mer**

**9 membres**
(4 femmes, 5 hommes)
**dont 4 à temps plein**

**22 agents**
(au 31/12/2024)

- 11 hommes / 11 femmes,
- 13 agents publics / 9 agents contractuels,
- 39 ans d'âge moyen.

# Rapport d’activité 2024

# Partie 1. L'état de la surveillance en 2024 : une stabilisation du nombre des personnes surveillées associée à une hausse modérée de la surveillance malgré des défis sécuritaires exceptionnels

*Ainsi que le prévoit l'article L. 833-9 du code de la sécurité intérieure (CSI), la Commission nationale de contrôle des techniques de renseignement (CNCTR) rend compte dans ses rapports publiés chaque année de l'accomplissement de sa mission tendant à veiller à ce que les techniques de renseignement soient mises en œuvre conformément au cadre légal les régissant. À cet effet, elle communique des informations aussi détaillées que le permet le secret de la défense nationale sur son activité de contrôle et fait état au public de ses constats sur l'utilisation que font les services des techniques de renseignement à l'endroit des personnes présentes sur le territoire national.*

*Mis en perspective sur une période quinquennale, ces éléments portent sur le nombre de personnes surveillées, sur les finalités*[1] *invoquées à l'appui des demandes de techniques de renseignement dont la commission est saisie ainsi que sur le nombre d'avis rendus sur ces demandes d'autorisation.*

1. Les dispositions de l'article L. 811-3 du code de la sécurité intérieure mentionnent sept finalités : au 1° de cet article, « l'indépendance nationale, l'intégrité du territoire et la défense nationale » (finalité 1), à son 2°, « les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère » (finalité 2), à son 3°, « les intérêts économiques, industriels et scientifiques majeurs de la France » (finalité 3), à son 4°, « la prévention du terrorisme » (finalité 4), à son 5°, « la prévention : a) des atteintes à la forme républicaine des institutions ; b) des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; c) des violences collectives de nature à porter gravement atteinte à la paix publique » (finalités 5a/5b/5c), à son 6°, « la prévention de la criminalité et de la délinquance organisées », et à son 7°, « la prévention de la prolifération des armes de destruction massive ».

*La commission rend par ailleurs compte du nombre d'avis préalables qu'elle a prononcés en 2024 sur les demandes relevant de la surveillance des communications électroniques internationales.*

*Les éléments statistiques présentés dans ce rapport sont issus d'un travail d'extraction et d'agrégation de données réalisé par la CNCTR conjointement avec le Groupement interministériel de contrôle (GIC), puis de fiabilisation des données.*

À l'instar de l'année 2023, l'année 2024 a été marquée par le niveau très élevé des menaces pesant sur la France dans un contexte de tensions géopolitiques intenses (guerre sur le sol européen, en Ukraine, depuis février 2022, conflit au Proche-Orient depuis octobre 2023…). S'est ajoutée à ce contexte **une situation exceptionnelle sur le plan intérieur soulevant des enjeux de sécurité forts avec, en particulier, l'organisation les Jeux olympiques et paralympiques de Paris 2024, précédés du relais de la flamme olympique dès mai 2024.** Toutefois, outre cet événement hors-norme, il y a également lieu de souligner **des niveaux de violence collective inédits en Nouvelle-Calédonie puis aux Antilles et enfin, en décembre 2024, la réouverture de la cathédrale Notre-Dame de Paris** ayant conduit à la présence dans la capitale de plusieurs dizaines de chefs d'État et de gouvernement.

Les pratiques des services de renseignement en matière de surveillance technique changent au gré des menaces et des instabilités mais aussi en fonction des évolutions technologiques, qui remettent parfois en cause l'intérêt de certaines techniques en raison d'une efficacité peu satisfaisante.

Dans ce contexte, le glissement déjà constaté au cours des années précédentes vers les techniques les plus intrusives s'est poursuivi en 2024 avec notamment **un recours de plus en plus important à**

**la technique, non contingentée, du recueil de données informatiques (RDI)**, prévue à l'article L. 853-2 du CSI. Pour autant, ce recours de plus en plus important aux techniques les plus intrusives ne **s'accompagne pas d'une baisse significative du recours aux techniques « historiques »** telles que les interceptions de sécurité, inscrites à l'article L. 852-1 du CSI.

Au total, malgré une année tout à fait exceptionnelle sur le plan des enjeux sécuritaires et une augmentation sensible de l'activité de certains services dans le contexte de l'organisation des Jeux olympiques et paralympiques de Paris 2024, la CNCTR constate **une stabilisation globale du nombre de personnes surveillées**, avec des tendances divergentes selon la finalité au titre de laquelle la surveillance est opérée (1.1). **Cette stabilisation se retrouve également dans le nombre de techniques de renseignement sollicitées**, même si elle ne doit pas masquer une **augmentation sensible des demandes portant sur les techniques les plus intrusives**, renforçant une tendance déjà observée depuis quelques années (1.2). Les finalités invoquées à l'appui de ces demandes conservent une répartition similaire à celles des années précédentes (1.3)

## 1.1. Une stabilisation du nombre des personnes surveillées qui ne doit pas masquer des tendances divergentes selon la finalité au titre de laquelle la surveillance est opérée

Comme elle le fait depuis son premier rapport d'activité, la commission a estimé le nombre de personnes ayant fait l'objet en 2024 d'au moins une technique de renseignement, parmi celles prévues aux chapitres I à III du titre V du livre VIII du CSI.

Ne sont pas prises en compte les autorisations d'accès aux données de connexion en temps différé qui se bornent à permettre l'identification d'abonnés et le recensement de numéros d'abonnement[2].

Après avoir augmenté de près de 15 % en 2023, **le nombre de personnes surveillées s'élève cette année à 24 308**, soit une augmentation de seulement 0,4 % par rapport à l'année 2023 et de 10,7 % par rapport à la période antérieure à la crise sanitaire liée à la pandémie de Covid-19.

| | 2020 | 2021 | 2022 | 2023 | 2024 | Evolution 2023/2024 | Evolution 2020/2024 |
|---|---|---|---|---|---|---|---|
| **Nombre de personnes surveillées** | **21 952** | **22 958** | **20 958** | **24 209** | **24 308** | **+ 0,4 %** | **+ 10,7 %** |
| **Au titre de la prévention du terrorisme** | **8 786** (40 % du total) | **7 826** (34,1 % du total) | **6 478** (30,9 % du total) | **6 962** (28,8 % du total) | **7 264** (29,9 % du total) | **+ 4,3 %** | **- 17,3 %** |
| **Au titre de la prévention de la criminalité et de la délinquance organisées** | **5 021** (22,9 % du total) | **5 932** (25,8 % du total) | **5 471** (26,1 % du total) | **7 058** (29,2 % du total) | **6 761** (27,8 % du total) | **- 4,2 %** | **+ 34,7 %** |
| **Au titre de la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure** | **3 238** (14,8 % du total) | **3 466** (15,1 % du total) | **2 692** (12,8 % du total) | **2 551** (10,5 % du total) | **2 528** (10,4 % du total) | **- 0,9 %** | **- 21,9 %** |

Comme souligné dans les rapports précédents, les résultats de ce calcul comportent une marge d'incertitude de l'ordre de 10 % (voir sur ce point le 8ème rapport d'activité de la commission p. 30)[3].

La stabilisation du nombre de personnes surveillées est, principalement, à mettre en lien avec le recentrage d'une partie de l'activité des services sur l'objectif de prévention du terrorisme dans

2. La CNCTR considère que les identifications d'abonnés et les recensements de numéros d'abonnement, prévus au deuxième alinéa de l'article L. 851-1 du CSI, constituent moins une mesure de surveillance à proprement parler qu'un préalable à des mesures de surveillance. De telles mesures commencent, du point de vue de la commission, dès l'obtention de « factures détaillées » de la personne concernée en application du premier alinéa du même article L. 851-1 du même code.

3. Le traitement des demandes de techniques de renseignement utilise différents applicatifs, ce qui conduit à agréger des données qui ne sont, encore aujourd'hui, pas complètement harmonisées. Par ailleurs, les demandes des services sont présentées par technique de renseignement mentionnée par le code de la sécurité intérieure et non par personne. En outre, les personnes visées ne sont pas toujours nommément ou précisément identifiées.

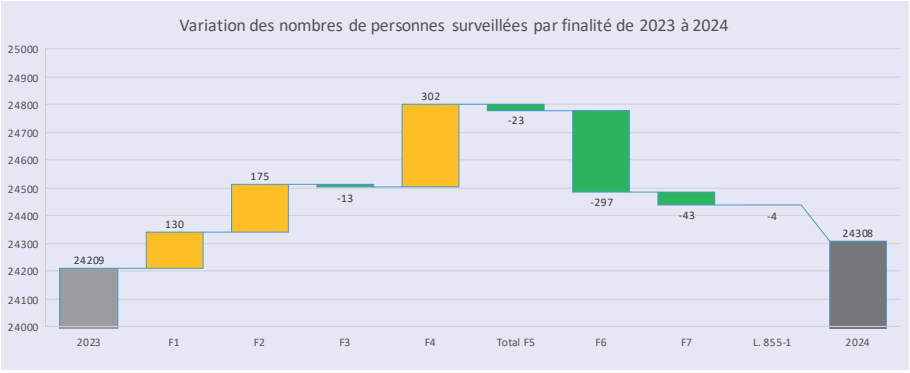
le contexte de l'organisation des Jeux olympiques et paralympiques de Paris 2024 (voir figures section 1.1.1).

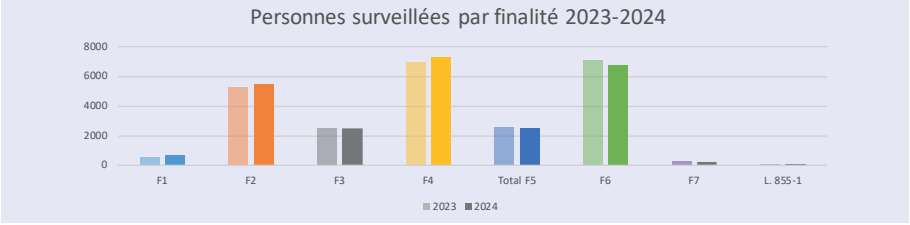
Ainsi, **l'année 2024 a été marquée par une intensification de l'investissement des services de renseignement dans la prévention du terrorisme, la prévention des ingérences, ainsi que dans la protection de l'indépendance nationale, de l'intégrité du territoire et de la défense nationale**. L'augmentation du nombre de personnes surveillées au titre de ces finalités s'accompagne d'une baisse du nombre de celles surveillées au titre de la prévention de la délinquance et de la criminalité organisées, même si dans les deux cas les variations sont modestes (1.1.1).

Par ailleurs, **la prévention des diverses formes d'activisme violent** (finalités mentionnées au 5° de l'article L. 811-3 du code de la sécurité intérieure), domaine où l'enjeu de protection de la vie privée se double d'un enjeu de protection des libertés d'expression, d'opinion, d'association ou encore de manifestation, **connaît pour la troisième année de suite une légère diminution** (1.1.2).

### 1.1.1. La prévention du terrorisme redevient en 2024 le premier motif de surveillance en nombre de personnes concernées

Les graphiques ci-dessous exposent à la fois la manière dont se répartit la variation du nombre de personnes surveillées selon les différentes finalités et l'évolution de ce nombre pour chacune de ces finalités entre 2023 et 2024.




(F1) : l'indépendance nationale, l'intégrité du territoire et la défense nationale ;

(F2) : les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

(F3) : les intérêts économiques, industriels et scientifiques majeurs de la France ;

(F4) : la prévention du terrorisme ;

(F5) : la prévention : a) des atteintes à la forme républicaine des institutions ; b) des actions tendant au maintien ou à la reconstitution de groupements dissous ; c) des violences collectives de nature à porter gravement atteinte à la paix publique ;

(F6) : la prévention de la criminalité et de la délinquance organisées ;

(F7) : la prévention de la prolifération des armes de destruction massive ;

L. 855-1 : finalité propre aux services de renseignement pénitentiaire, prévue à l'article L. 855-1 du code de la sécurité intérieure, tenant à la prévention des évasions et à la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

L'année 2023 avait vu une augmentation sensible du nombre de personnes surveillées au titre de la prévention de la criminalité et de la délinquance organisée (+ 29 % par rapport à 2022), conduisant à faire de cette finalité le premier motif de surveillance en nombre de personnes concernées. Sur la même période, le nombre de personnes surveillées au titre de la prévention du terrorisme avait connu une augmentation plus mesurée (+ 7,5 %).

En 2024, dans le **contexte d'un renforcement des menaces tant exogènes qu'endogènes** accompagnant la tenue des Jeux olympiques et paralympiques, **la finalité mentionnée au 4° de l'article L. 811-3 du CSI redevient le premier motif de surveillance tant en nombre de personnes concernées que de techniques mises en œuvre** (voir point 1.3 ci-dessous). Corrélativement, le nombre de personnes surveillées au titre de la finalité mentionnée au 6° du même article connaît une baisse, qui reste mesurée (- 4,2 %).

Au-delà, la prévention de la criminalité et de la délinquance organisées est le motif de surveillance qui a connu la plus grande augmentation en nombre de personnes concernées au cours des cinq dernières années (+ 18,8 %, correspondant à 6 761 personnes suivies à ce titre en 2024 contre 5 693 en 2019).

**Une situation géopolitique internationale très instable** explique par ailleurs la **poursuite de l'augmentation du nombre de personnes surveillées au titre de la finalité tenant à la défense et à la promotion des intérêts majeurs de la politique étrangère**, de l'exécution des engagements européens et internationaux de la France et la **prévention de toute forme d'ingérence étrangère** (+ 3,3 % entre 2023 et 2024).

### 1.1.2. Le nombre de personnes surveillées au titre de la prévention des différentes formes d'activisme violent continue de baisser

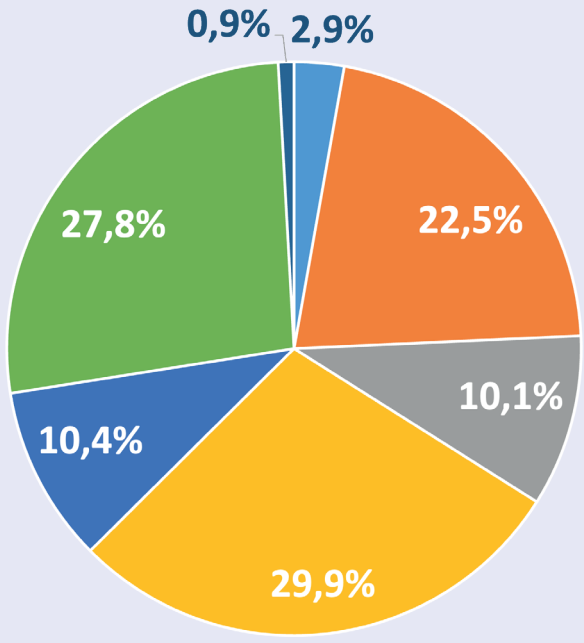
Dans le prolongement de la tendance relevée depuis 2021, le recul du nombre de personnes surveillées au titre des finalités mentionnées au 5° de l'article L. 811-3 du code de la sécurité intérieure se confirme en 2024 avec une baisse de 0,9 % par rapport à 2023 (à comparer à la baisse de 5,2 % entre 2022 et 2023). Le **nombre de personnes surveillées au titre de cette finalité atteint son plus bas niveau depuis 2018**[4].

Comme en 2023, cette évolution est liée à la poursuite de l'augmentation sensible du nombre de demandes de renseignements complémentaires formées par la commission (voir point 1.2.4 ci-dessous) qui ont contribué à poursuivre le dialogue instauré depuis 2022 avec les services sur les contours de cette finalité[5]. Ces échanges ont permis de mieux identifier les personnes justifiant un suivi, conduisant corrélativement à une stabilisation du taux d'avis défavorables rendus en la matière.

Par ailleurs, le nombre de personnes surveillées au titre de la défense et de la promotion des intérêts économiques, industriels et économiques majeurs de la France se stabilise autour de son niveau constaté avant la crise sanitaire liée à la pandémie de Covid-19.

4. 2 116 personnes étaient surveillées à ce titre en 2021 (6ème rapport d'activité 2021 de la CNCTR, p. 73).
5. Voir sur ce point l'étude relative à la surveillance des extrémismes violents figurant dans le 7ème rapport d'activité 2022 de la CNCTR, p. 75 et suivantes.

## La répartition des personnes surveillées selon les finalités motivant leur surveillance




- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

*Nota : Une même personne pouvant être surveillée au titre de plusieurs finalités, l'agrégat des différents pourcentages présentés dépasse 100 %*

## 1.2. Une augmentation modérée du nombre de demandes de techniques de renseignement avec néanmoins un renforcement du recours aux techniques les plus intrusives

Malgré un haut niveau de menaces et le contexte de l'organisation des Jeux olympiques et paralympiques, **le nombre de demandes tendant à la mise en œuvre de techniques de renseignement sur le territoire national a connu une hausse modérée de 3 % par rapport à l'année précédente pour atteindre 98 883 demandes**[6]. Corrélée à la stabilisation du nombre de personnes ayant fait l'objet d'une surveillance, cette hausse traduit une légère augmentation du nombre moyen de techniques sollicitées pour chaque personne surveillée.

Le constat de cette relative stabilité du nombre de techniques sollicitées peut s'expliquer par le fait que si l'activité de certains services a augmenté en amont et pendant la période des Jeux olympiques et paralympiques, cette augmentation a d'abord reposé sur une réaffectation temporaire d'une partie de leurs moyens humains et techniques aux fins d'anticiper les menaces susceptibles de viser cet événement.

La CNCTR émet un avis sur chaque demande visant à mettre en œuvre une technique de renseignement sur le territoire national avant que le Premier ministre ne prenne une décision autorisant ou refusant cette mise en œuvre[7]. Elle doit se prononcer dans un délai de vingt-quatre heures lorsqu'une demande relève de la

6. Ce chiffre recouvre les techniques dites « individualisées » et n'inclut donc pas les demandes fondées sur l'article L. 851-3 du code de la sécurité intérieure (technique dite de l'algorithme), ni les transmissions entre services relevant d'une autorisation de la commission.

7. Voir le 7ème rapport d'activité 2022 de la CNCTR, p. 132.

compétence d'un membre ayant la qualité de magistrat[8] et statuant seul. Ce délai est porté à soixante-douze heures lorsque la demande nécessite un examen en formation collégiale, plénière ou restreinte[9]. La commission s'attache à respecter ces délais. Une procédure dite « prioritaire » a par ailleurs été mise en place pour répondre aux besoins opérationnels nécessitant un traitement très urgent des demandes[10].

Les avis émis se répartissent comme indiqué dans le tableau ci-dessous. Ces chiffres incluent l'ensemble des demandes présentées par les services de renseignement au cours des années 2020 à 2024[11]. Ils permettent de saisir les évolutions de la façon dont les services recourent à chaque catégorie de techniques sur cinq ans ainsi que d'une année sur l'autre.

| | 2020 | 2021 | 2022 | 2023 | 2024 | Évolution 2023 / 2024 | Évolution 2020 / 2024 |
|---|---|---|---|---|---|---|---|
| **Accès aux données de connexion en temps différé** (Identification d'abonnés ou recensement de numéros d'abonnement) (article L. 851-1 du code de la sécurité intérieure) | 30 758 | 32 254 | 31 427 | 33 657 | 34 612 | + 2,8 % | + 12,5 % |
| **Accès aux données de connexion en temps différé** (Autres demandes, dont celles de « factures détaillées ») (article L. 851-1 du code de la sécurité intérieure) | 18 006 | 19 974 | 19 263 | 21 430 | 22 493 | + 5 % | + 24,9 % |
| **Accès aux données de connexion en temps réel** (article L. 851-2 du code de la sécurité intérieure) | 1 644 | 1 534 | 1 175 | 763 | 731 | - 4,2 % | - 55,5 % |

8. Membres mentionnés aux 2° et 3° de l'article L. 831-1 du code de la sécurité intérieure.

9. En vertu des dispositions de l'article L. 832-3 du code de la sécurité intérieure, les formations collégiales de la commission ont notamment à connaître de toute question nouvelle ou sérieuse. La formation collégiale plénière se réunit au moins une fois par mois et est en particulier compétente pour connaître des demandes relatives aux professions protégées au sens de l'article L. 821-7 du CSI.

10. Cette procédure permet à la commission de rendre des avis dans un délai généralement inférieur à une heure.

11. Les données figurant dans le tableau n'incluent pas les demandes non-individualisées et/ou relevant des mesures de surveillance des communications électroniques internationales ce qui recouvre les demandes ayant trait à la technique dite de l'algorithme prévue à l'article L. 851-3 du code de la sécurité intérieure, les demandes de transmissions de renseignement subordonnées à un avis préalable de la commission mentionnées au II de l'article L. 822-3 du même code ou les autorisations d'exploitation mentionnées à son article L. 854-2 (voir respectivement p. 42 et p. 49 ci-dessous).

| | 2020 | 2021 | 2022 | 2023 | 2024 | Évolution 2023 / 2024 | Évolution 2020 / 2024 |
|---|---|---|---|---|---|---|---|
| **Géolocalisations en temps réel** (article L. 851-4 du code de la sécurité intérieure) | 8 394 | 9 920 | 10 901 | 10 982 | 9 909 | - 9,8 % | + 18 % |
| **Interceptions de sécurité via le GIC** (I de l'article L. 852-1 du code de la sécurité intérieure) | 12 891 | 12 736 | 12 798 | 13 021 | 14 316 | + 9,9 % | + 11,1 % |
| **Interceptions des communications par *IMSI catcher*** (II de l'article L. 852-1 du code de la sécurité intérieure) | 0 | 0 | 0 | 0 | 0 | - | - |
| **Interceptions de sécurité sur les réseaux exclusivement hertziens** (article L. 852-2 du code de la sécurité intérieure) | 0 | 3 | 5 | 10 | 5 | - 50 % | - |
| **Interceptions de correspondances émises ou reçues par la voie satellitaire** (article L. 852-3 du code de la sécurité intérieure) | 0 | 0 | 0 | 0 | 1 | - | - |
| **Localisations des personnes ou des objets** (« Balisages ») (article L. 851-5 du code de la sécurité intérieure) | 1 598 | 2 006 | 1 951 | 2 084 | 2 065 | - 0,9 % | + 29,2 % |
| **Recueils de données de connexion par *IMSI catcher*** (article L. 851-6 du code de la sécurité intérieure) | 311 | 583 | 641 | 607 | 616 | + 1,5 % | + 98,1 % |
| **Captations de paroles prononcées à titre privé et captations d'images dans un lieu privé** (article L. 853-1 du code de la sécurité intérieure) | 1 564 | 2 138 | 3 314 | 3 802 | 3 912 | + 2,9 % | + 150,1 % |
| **Recueils et captations de données informatiques** (article L. 853-2 du code de la sécurité intérieure) | 2 418 | 3 758 | 4 260 | 4 493 | 5 715 | + 27,2 % | + 136,4 % |
| **Introductions dans des lieux privés** (article L. 853-3 du code de la sécurité intérieure) | 2 021 | 2 682 | 3 767 | 4 053 | 4 508 | + 11,2 % | + 123,1 % |
| **Ensemble des techniques de renseignement** | 79 605 | 87 588 | 89 502 | 94 902 | 98 883 | + 4,2 % | + 24,3 % |

### 1.2.1. La tendance des services de renseignement à avoir recours à des techniques de surveillance plus intrusives se confirme et se renforce en 2024

La hausse modérée du nombre de demandes de mise en œuvre de techniques relevée en 2024 ne remet pas en cause la dynamique constatée depuis plusieurs années d'un recours de plus en plus fréquent aux techniques les plus intrusives.

En effet, **la hausse la plus notable en 2024 concerne la technique de recueil et de captation de données informatiques (RDI)[12] pour laquelle le nombre de demandes augmente de plus de 27 % en 2024 par rapport à l'année précédente**, après une augmentation de 5,5 % en 2023 et de 13,4 % en 2022.

Cette hausse ne peut être expliquée uniquement par le contexte exceptionnel de l'organisation des Jeux olympiques et paralympiques. La CNCTR y voit une tendance bien installée du recours croissant à cette technique notamment pour pallier les limites des interceptions de sécurité. Le recours au RDI peut en effet permettre de surmonter les difficultés liées à l'usage toujours plus important de canaux chiffrés pour communiquer. En cinq années, le nombre de demandes de RDI a ainsi bondi de plus de 136 % entre 2020 et 2024.

Pour les autres techniques les plus intrusives, l'augmentation des demandes est moins marquée mais suit une dynamique de croissance qui ne s'infléchit pas depuis 2020.

Ainsi, les techniques de **captation de paroles prononcées à titre privé ou de captation d'images dans un lieu privé** ont augmenté de 2,9 % au cours de l'année 2024, portant l'augmentation à plus de 150 % sur les cinq dernières années.

12. Voir les dispositions de l'article L. 853-2 du CSI.

En cohérence avec l'augmentation du recours aux techniques de recueil de données informatiques ou de captation de paroles ou d'images, les demandes d'**introduction dans des lieux privés**, qui ne constitue pas une technique de surveillance en tant que telle, mais une technique « support » nécessaire à la mise en œuvre de techniques de renseignement proprement dites, ont connu une augmentation importante, de plus de 11 % en 2024.

Par ailleurs, après une baisse modérée en 2023, les demandes de **recueil de données de connexion par *IMSI catcher*** ont très légèrement augmenté de 1,5 % en 2024, mettant en évidence une stabilisation du recours à cette technique par les services au cours des quatre dernières années. Cette stabilité est sans doute à mettre en lien avec le fait qu'à l'instar des interceptions de sécurité, cette technique est soumise à un contingentement en vertu des dispositions de l'article L. 851-6 du CSI.

Enfin, une nouvelle autorisation de mise en œuvre d'un traitement automatisé destiné à détecter des connexions susceptibles de révéler une menace terroriste (technique dite de l'**algorithme**, prévue à l'article L. 851-3 du CSI[13]) a été délivrée en 2024, portant à six le nombre d'algorithmes autorisés depuis l'ouverture de cette technique aux services de renseignement en 2015. L'un d'entre eux a été abandonné en 2024. La faculté ouverte par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement d'étendre la technique de l'algorithme aux adresses complètes de ressources utilisées sur internet (***Uniform Resource Locator***, URL)[14], de même que celle de recourir à la technique pour d'autres finalités que celle tenant à la prévention du terrorisme, ouverte par la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France[15] n'ont toutefois pas encore été mises en œuvre.

13. Voir l'étude consacrée à cette technique p. 98 - Étude – L'algorithme : d'une vision fantastique à la réalité juridique.

14. Voir l'article 15 de la loi qui a modifié le I de l'article L. 851-3 du code de la sécurité intérieure.

15. Voir l'article 6 de la loi qui modifie temporairement, jusqu'au 1er juillet 2028, les dispositions de l'article L. 851-3 du code de la sécurité intérieure afin d'ouvrir la technique aux finalités mentionnées aux 1° et 2° de l'article L. 811-3 du même code afin de prévenir les ingérences étrangères et les menaces pour la défense nationale.

### 1.2.2. Le recours aux techniques « traditionnelles » moins intrusives ne faiblit pas pour autant

Malgré le recours à des techniques plus intrusives et tout particulièrement au RDI, les techniques de renseignement dites traditionnelles ne sont pas délaissées par les services de renseignement et sont au contraire confortées dans leur statut de techniques de première intention, dans la mesure où elles permettent notamment de justifier l'intérêt présenté par une personne concernée par une surveillance ou de mieux appréhender son environnement.

***Poursuite de l'augmentation des demandes d'accès aux données de connexion***

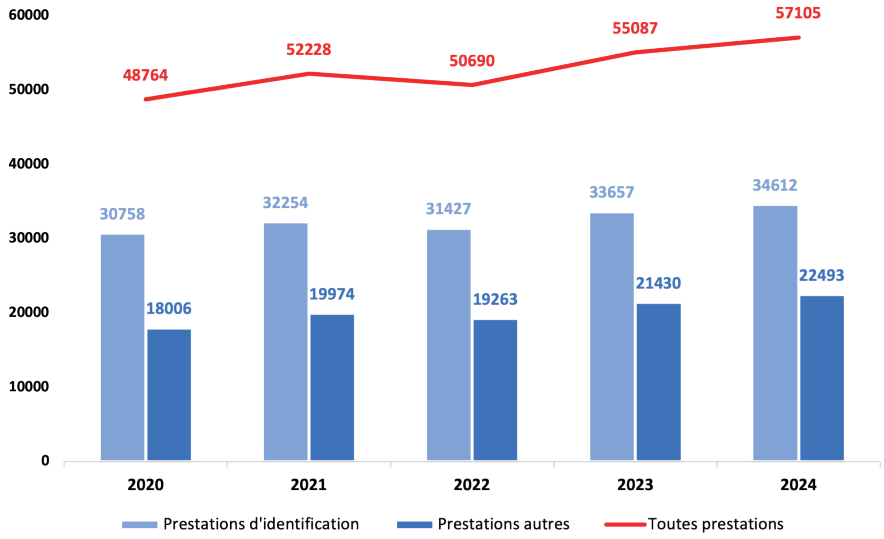
Après avoir connu un infléchissement en 2022, le nombre de demandes d'accès aux données de connexion en temps différé continue sa progression en 2024 (+ 3,7 % par rapport à 2023). Les demandes portant sur ces accès, moins intrusifs que les autres techniques prévues par le code de la sécurité intérieure, représentent ainsi plus de la moitié des demandes de techniques de renseignement formées par les services en 2024.

Sur ce point, l'année écoulée ne constitue pas une rupture par rapport aux années précédentes. En effet, comme cela a été noté dans le rapport d'activité de la commission pour l'année 2023, les accès aux données de connexion sont une technique de surveillance de première intention permettant aux services de mieux connaître l'environnement de la personne visée.

Cette part importante des demandes d'accès aux données de connexion dans l'ensemble des demandes de techniques de renseignement formées par les services est un indicateur important

à suivre. Sa stabilité montre en effet que les services ont intégré et continuent à appliquer un principe de subsidiarité dans le recours aux techniques de renseignement, consistant notamment à progresser par étapes dans la surveillance d'une personne. Or, la première étape de la surveillance réside encore majoritairement par l'obtention de ces données de connexion, très utiles pour commencer une enquête et apprécier la nécessité de la poursuivre, mais moins révélatrices de la vie privée des personnes visées.

**Évolution de la répartition des demandes d'accès aux données de connexion entre 2020 à 2024**




En revanche, les demandes d'**accès aux données de connexion en temps réel** continuent de diminuer : - 4,2 % en 2024, après un recul de 35 % en 2023 et de 23 % en 2022, semblant conforter l'analyse selon laquelle la limitation de cette technique à la finalité tenant à la prévention du terrorisme conduit les services à privilégier d'autres techniques, parfois plus intrusives, pour les autres finalités prévues par le code de la sécurité intérieure.

### *Une augmentation du recours aux interceptions de sécurité*

Même si leur apport est moindre que par le passé en termes de renseignement au sens strict, un des faits notables de l'année 2024 réside dans **l'augmentation sensible des demandes d'interceptions de sécurité** (les « écoutes téléphoniques »), mises en œuvre via le Groupement interministériel de contrôle (GIC) pour le compte des services de renseignement, **de près de 10 % en 2024** par rapport à l'année précédente, après une augmentation plus modérée de 1,7 % en 2023.

Cette tendance met en évidence que la technique demeure d'intérêt pour les services afin d'améliorer leur connaissance d'une personne surveillée et de préparer le recours à d'autres techniques plus intrusives si l'intérêt qu'elle présente se vérifie. Il y a lieu à cet égard de souligner que pour la première fois depuis 2019, le Premier ministre a augmenté en 2024, à titre temporaire, puis tout début 2025, de façon pérenne, le contingent d'interceptions pouvant être mises en œuvre simultanément[16].

## UNE ÉVOLUTION DU CONTINGENT DES INTERCEPTIONS DE SÉCURITÉ POUR LA PREMIÈRE FOIS DEPUIS 2019

Les interceptions de sécurité, prévues à l'article L. 852-1 du code de la sécurité intérieure, font partie des quatre techniques dites « domestiques »[17] soumises au principe du contingentement en application duquel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par décision du Premier ministre, prise après avis de la CNCTR.

Ce principe de contingentement vise à garantir que les services ne recourent aux techniques concernées que ***« dans les seuls cas de nécessité d'intérêt public prévus par la loi »***[18].

16. Voir encadré ci-dessous.

17. Les autres techniques domestiques soumises à contingentement sont l'accès aux données de connexion en temps réel (article L. 851-2 du CSI), le recueil de données de connexion par IMSI catcher (article L. 851-6 du CSI) et l'interception de correspondance par la voie satellitaire (article L. 852-3 du CSI).

18. Voir article L. 801-1 du CSI.

Déjà prévu par la loi n° 91-946 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, le contingent des interceptions de sécurité pouvant être accordé simultanément n'avait pas été modifié à la date d'entrée en vigueur de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement et était resté fixé à 2 700. Par la suite, il a été augmenté à trois reprises en 2017, 2018 et 2019, pour être finalement porté à 3 800.

En 2024, pour la première fois depuis 2019, la commission a été saisie par le Premier ministre de deux projets d'augmentation du contingent applicable aux interceptions de sécurité :

- en début d'année, lui a été soumis un projet d'augmentation temporaire de ce contingent dans le contexte de l'organisation des Jeux olympiques et paralympiques 2024,

- puis en fin d'année, un projet d'augmentation pérenne s'appuyant sur le niveau élevé de la menace à laquelle est exposée la France.

Par deux délibérations classifiées, la CNCTR a estimé avéré, d'une part, le besoin d'augmenter temporairement le contingent fixé en 2019 dans le contexte exceptionnel des Jeux olympiques et paralympiques, de nature à exacerber un niveau de menace déjà très élevé. D'autre part, elle a admis qu'au-delà des incidences de cet événement particulier, le niveau de menace tant exogène qu'endogène pesant sur le pays justifiait de façon pérenne une augmentation de ce contingent, mais dans une proportion moindre.

### Évolution du contingent des interceptions de sécurité depuis 2015

| Ministère chargé : | 2015 | 2017 | 2018 | 2019 | 2024 (contingent temporaire) | À compter du 1er octobre 2024 | 2025 |
|---|---|---|---|---|---|---|---|
| de l'intérieur | 2 235 | 2 545 | 3 000 | 3 050 | 3 750 | 3 100 | 3 350 |
| de la défense | 320 | 320 | 400 | 550 | 600 | 550 | 600 |
| de l'économie et du budget (douanes, Tracfin) | 145 | 145 | 150 | 150 | 130 | 130 | 130 |
| de la justice | - | 30 | 50 | 50 | 20 | 20 | 20 |
| Total | 2 700 | 3 040 | 3 600 | 3 800 | 4 500 | 3 800 | 4 100 |

Comme en 2023, l'**utilisation des techniques de localisation des personnes ou des objets** (les « balises ») demeure stable sur les cinq dernières années avec un volume de l'ordre de 2 000 demandes par an.

Par ailleurs, si les demandes de **géolocalisation en temps réel** apparaissent comme ayant sensiblement diminué, de près de 10 % en 2024, cette évolution doit être relativisée. En effet, fin 2023, un changement de logiciel a été opéré pour la saisine de ces demandes permettant aux services de ne former qu'une seule demande de géolocalisation pour les différents identifiants techniques appartenant à une même personne au lieu d'une demande par identifiant. La baisse du nombre de demandes constatée en 2024 ne traduit donc pas un moindre recours à la technique.

**De façon générale, ces évolutions mettent en évidence que les services de renseignement adaptent les modalités de la surveillance aux contraintes imposées par l'expansion des moyens de communication assurant un haut niveau de confidentialité.**

À cet égard, il y a lieu de relever que la première demande d'**interceptions émises ou reçues par la voie satellitaire**, fondée sur les nouvelles dispositions de l'article L. 852-3 du code de la sécurité intérieure introduites par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement[19], a été présentée au cours de l'année 2024 (voir encadré ci-dessous).

19. Voir l'article 13 de la loi instaurant une expérimentation jusqu'au 31 juillet 2025.

## LES INTERCEPTIONS PAR LA VOIE SATELLITAIRE : CONCRÉTISATION DE L'EXPÉRIMENTATION

La loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, dite loi PATR, a introduit dans le code de la sécurité intérieure (CSI) un nouvel article L. 852-3 permettant, au titre des finalités mentionnées aux 1°, 2°, 4° et 6° de son article L. 811-3, de recourir à un appareil ou un dispositif technique afin d'intercepter les correspondances émises ou reçues par la voie satellitaire, « lorsque cette interception ne peut être mise en œuvre sur le fondement du I de l'article L. 852-1 », c'est-à-dire quand le recours aux écoutes téléphoniques n'est pas possible pour des motifs opérationnels ou de confidentialité.

L'article 13 de la loi du 30 juillet 2021 a prévu que ces dispositions seront applicables jusqu'au 31 juillet 2025 et que le gouvernement adresse au Parlement un rapport d'évaluation sur l'application de ces dispositions au plus tard six mois avant cette échéance.

À l'instar notamment des interceptions de sécurité prévues par les dispositions de l'article L. 852-1 du CSI, les interceptions par la voie satellitaire sont soumises au principe du contingentement. Or, en l'absence de fixation du nombre maximal d'autorisations pouvant être accordées simultanément, cette nouvelle technique n'avait pas été mise en œuvre jusqu'en 2023.

L'avancement des phases de test a conduit à ce que la commission puisse être saisie en 2024 d'un projet de fixation du contingent applicable aux interceptions de sécurité par voie satellitaire.

Par une délibération classifiée, la CNCTR a estimé que la proposition du gouvernement de fixer ce contingent à 20 autorisations simultanées était justifiée et adaptée à la poursuite de l'expérimentation en situation opérationnelle.

En pratique, une autorisation a été délivrée au cours de l'année 2024.

La proposition de loi visant à sortir la France du piège du narcotrafic, adoptée par le Sénat le 28 avril 2025 et par l'Assemblée nationale le 29 avril 2025, comporte un article 8 *bis* qui prolonge l'expérimentation jusqu'au 31 décembre 2028[20].

### 1.2.3. Une stagnation du nombre de demandes d'autorisation d'exploitation en matière de surveillance des communications électroniques internationales

La CNCTR a rendu 3 942 avis en 2024 sur des demandes tendant à **l'exploitation de communications internationales** contre 3 981 en 2023. Ainsi, après une légère augmentation de ce nombre d'avis en 2023 (+ 7 %), une stagnation (- 1 %) a été observée au cours de l'année écoulée.

| | 2020 | 2021 | 2022 | 2023 | 2024 | Evolution 2023/2024 | Evolution 2020/2024 |
|---|---|---|---|---|---|---|---|
| **Nombre d'avis rendus en matière de surveillance des communications électroniques internationales** | **4 316** | **4 374** | **3 715** | **3 981** | **3 942** | **- 1 %** | **- 8,7 %** |

20. En l'état de la numérotation du texte adopté le 28 et 29 avril par le Sénat et par l'Assemblée nationale. Le texte a fait l'objet de trois saisines du Conseil constitutionnel le 12 mai 2025 (2025-885 DC). La décision du Conseil constitutionnel n'est pas encore intervenue à la date de finalisation du présent rapport.

## CADRE JURIDIQUE DE LA SURVEILLANCE INTERNATIONALE

La surveillance des communications électroniques internationales est régie par les dispositions des articles L. 854-1 à L. 854-9 du code de la sécurité intérieure (CSI). Ces dernières prévoient que les services spécialisés de renseignement peuvent être autorisés à exploiter les communications émises ou reçues à l'étranger, interceptées sur les réseaux de communications électroniques désignés par le Premier ministre.

Ces autorisations « d'exploitation » sont délivrées par le Premier ministre, après avis de la CNCTR. Plusieurs catégories d'autorisation sont prévues, selon l'objet et le périmètre de la surveillance envisagée. Il peut s'agir de surveiller les communications émises ou reçues au sein d'une zone géographique, par une organisation, par un groupe de personnes ou par une seule personne.

Quelle que soit leur nature, ces autorisations d'exploitation ne peuvent être fondées que sur les finalités énumérées à l'article L. 811-3 du CSI applicables à la surveillance intérieure.

Sauf exceptions expressément prévues par la loi, la surveillance individuelle des communications de personnes utilisant des numéros ou des identifiants « nationaux » (c'est-à-dire de communications « françaises ») est interdite. Si de telles communications venaient à être interceptées, elles devraient être immédiatement détruites.

### 1.2.4. Une augmentation sensible des demandes de renseignements complémentaires faites aux services de renseignement qui conduit à une stabilisation du taux d'avis défavorables

Les progrès en matière d'appréhension du cadre légal par les services, doivent être mis en perspective avec la poursuite d'une **augmentation sensible du nombre de demandes de renseignements complémentaires adressés par la commission aux services de renseignement**. En effet, ces demandes, toutes techniques confondues, ont augmenté, passant de 2,9 % du nombre total de demandes en 2023 (2 797 demandes de RC) à 3,3 % du total de demandes pour l'année 2024 (3 307 demandes de RC), soit une augmentation de 18,2 % de demandes de renseignements complémentaires entre 2023 à 2024.

Les demandes de renseignements complémentaires constituent une occasion d'échange entre la commission et les services de renseignement, et favorisent une meilleure compréhension du cadre légal et des attentes de la CNCTR par ces derniers.

Ainsi, malgré une **augmentation du nombre de demandes de techniques de renseignement** adressées à la commission cela n'a **pas conduit à une augmentation significative des avis défavorables rendus par la commission**.

En 2024 comme en 2023, ce taux s'établit à 0,8 % toutes techniques confondues (775 avis défavorables en 2023 contre 803 en 2024).

Si on retranche les avis rendus sur les demandes de données de connexion, ce taux d'avis défavorables augmente très légèrement passant de 1,2 % à 1,3 %. Le nombre d'avis défavorables a ainsi augmenté de 9,3 % en 2024 par rapport à 2023, alors que sur la même période les demandes, hors données de connexion, ont augmenté d'un peu moins de 5 %.

| | 2023 | 2024 | Évolution 2023 / 2024 |
|---|---|---|---|
| **Techniques de renseignement (hors données techniques de connexion)** | | | |
| **Avis rendus** | **39 815** | **41 778** | **4,9 %** |
| **Demandes de renseignements complémentaires** | **1 373** (soit 3,4 % du total) | **1 609** (soit 3,9 % du total) | **+ 17,2 %** (0,5 pt) |
| **Avis défavorables** | **496** (soit 1,2 % du total) | **542** (soit 1,3 % du total) | **+ 9,3 %** (0,1 pt) |
| **Données techniques de connexion** | | | |
| **Avis rendus** | **55 087** | **57 105** | **3,7 %** |
| **Demandes de renseignements complémentaires** | **1 424** (soit 2,6 % du total) | **1 698** (soit 3 % du total) | **+ 19,2 %** (0,4 pt) |
| **Avis défavorables** | **279** (soit 0,5 % du total) | **261** (soit 0,5 % du total) | **- 6,5 %** (0 pt) |
| **Toutes techniques de renseignements confondues** | | | |
| **Avis rendus** | **94 902** | **98 883** | **4,2 %** |
| **Demandes de renseignements complémentaires** | **2 797** (soit 2,9 % du total) | **3 307** (soit 3,3 % du total) | **+ 18,2 %** (0,4 pt) |
| **Avis défavorables** | **775** (soit 0,8 % du total) | **803** (soit 0,8 % du total) | **+ 3,6 %** (0 pt) |

Parallèlement, le contexte de l'organisation des Jeux olympiques et paralympiques et de la mobilisation subséquente des services pour prévenir les menaces susceptibles de peser sur cet événement a été l'occasion pour la commission de renforcer une pratique initiée depuis quelques années, sur certaines thématiques, consistant à demander aux services de venir présenter au collège leur stratégie de surveillance technique : objectif poursuivi, choix des cibles et des techniques. Ces échanges présentent un avantage pour la commission aussi bien que pour les services. Du point de vue de la commission, ils permettent de mieux appréhender la démarche du service et de contextualiser ses demandes dans le cadre plus général du suivi d'une personne ou d'une thématique. Ces

échanges sont également l'occasion d'alerter les services sur la fragilité juridique éventuelle de demandes qui ne seraient pas suffisamment fondées avant même qu'elles ne soient soumises. Pour les services, ces échanges permettent de comprendre les attentes de la commission et renforcent leur capacité à lui présenter des demandes fondées sur des éléments de motivation solides. La commission entend poursuivre et approfondir ces échanges constructifs en 2025.

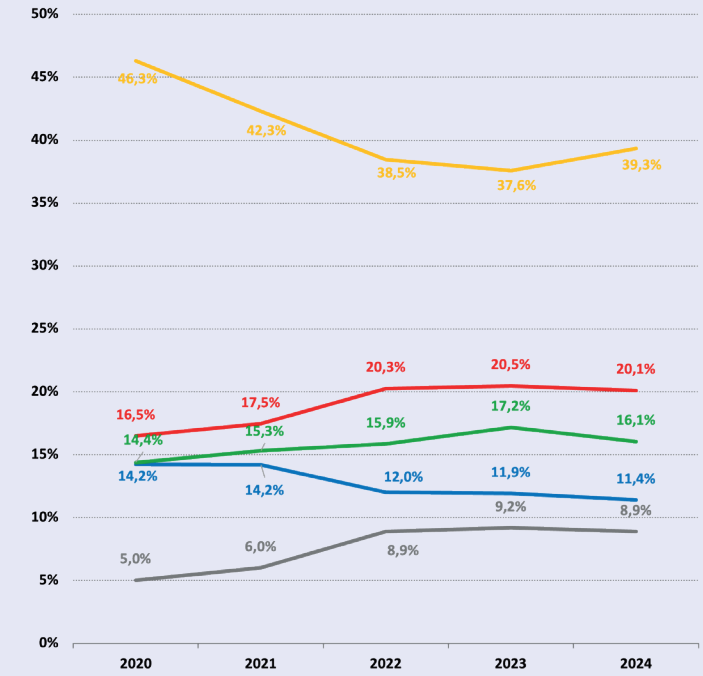
## 1.3. La répartition des demandes de techniques de renseignement par finalité demeure très similaire à celle constatée les années précédentes, malgré une augmentation du nombre de demandes motivées par la prévention du terrorisme

Ainsi que cela a été rappelé à plusieurs reprises dans les précédents rapports d'activité de la commission, les techniques de renseignement ne peuvent être mises en œuvre que pour la défense ou la promotion des intérêts fondamentaux de la Nation, limitativement énumérés à l'article L. 811-3 du code de la sécurité intérieure.

Même si depuis la création de la CNCTR, la **prévention du terrorisme** a toujours été le fondement légal le plus fréquemment invoqué à l'appui des demandes de techniques, le pourcentage de demandes fondées sur cette finalité avait néanmoins régressé. L'année 2024 inverse cette tendance de façon modérée, puisque la proportion de demandes fondées sur la prévention du terrorisme augmente de 1,7 % par rapport à l'année 2023. Plus de 39 % des demandes de techniques de renseignement ont ainsi été motivées sur ce fondement légal au cours de l'année 2024.

L'organisation des Jeux olympiques et paralympiques apparaît comme une des principales causes expliquant cette évolution dès lors que le risque d'actions violentes à caractère terroriste représentait l'une des principales menaces pesant sur cet événement et qu'il a donc constitué une priorité pour les services de renseignement concernés par ces enjeux. Cependant, au-delà et comme les années précédentes, la menace terroriste s'est maintenue à un niveau très élevé tout au long de l'année.

## Évolution du nombre de demandes par finalité les motivant entre 2020 et 2024



S'agissant des autres finalités, l'année 2024 n'a pas conduit à constater de rupture ou d'évolution notable.

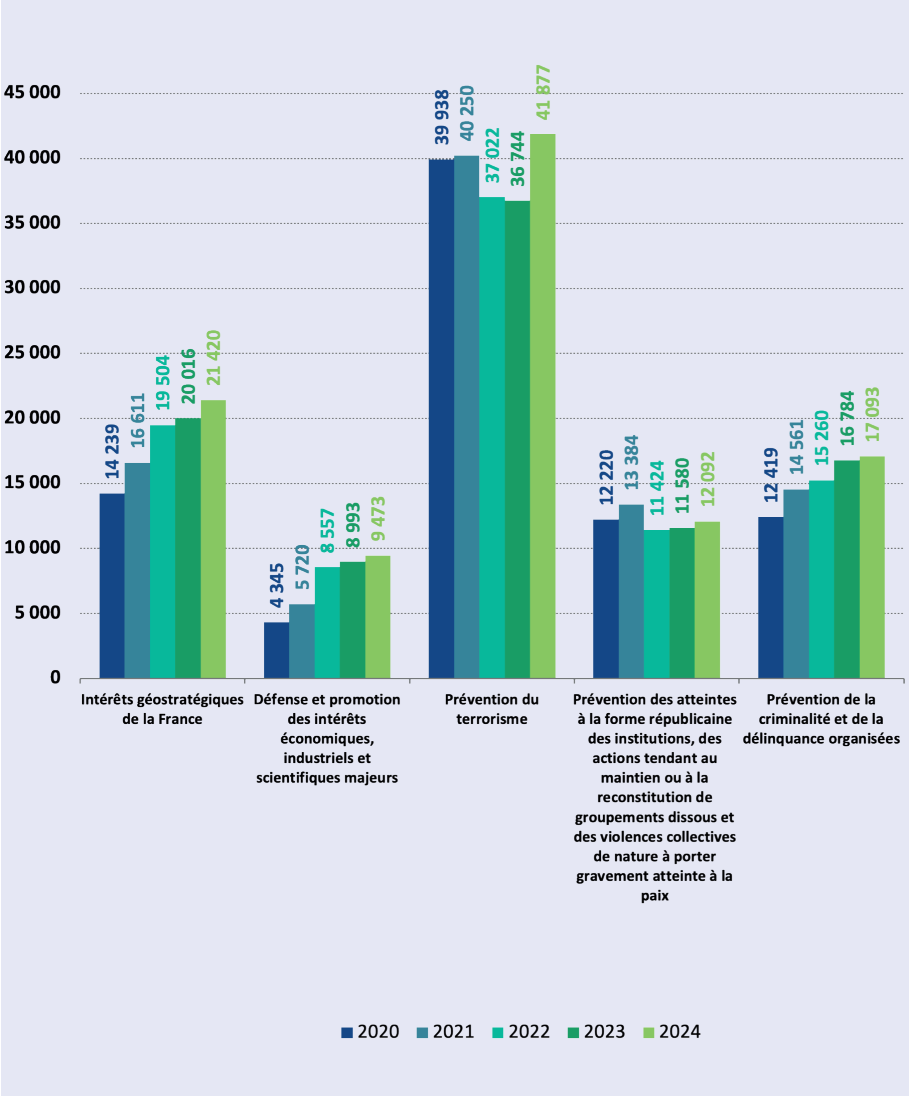
Avec un ratio de 20,1 %, les **finalités relevant des intérêts géostratégiques de la France** (indépendance et défense nationales, intérêts majeurs de la politique étrangère et prévention de toute forme d'ingérence étrangère, lutter contre la prolifération d'armes de destruction massive) demeurent le deuxième fondement légal le plus fréquemment invoqué avec une évolution stable (ce ratio était 20,5 % en 2023). Les efforts des services sur ces thématiques ont en effet été maintenus dans un contexte d'instabilité géopolitique croissante.

La part de la finalité tenant à la **prévention de la délinquance et de la criminalité organisées** régresse en 2024 par rapport à 2023, de 17,2 % à 16,1 % mais demeure très nettement le troisième fondement légal invoqué au soutien de demandes de techniques (à distinguer du nombre de personnes faisant l'objet d'une surveillance sur le fondement de cette finalité, voir point 1.1 ci-dessus). Ce léger recul ne résulte pas d'un moindre intérêt des services pour cette finalité, mais de la part un peu plus importante reprise par la finalité tenant à la prévention du terrorisme dans le contexte particulier de l'année 2024.

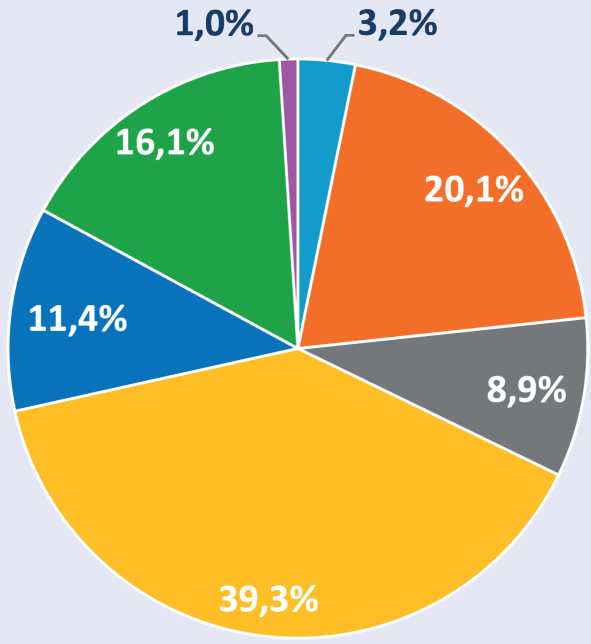
Ensuite, malgré une situation politique interne marquée par l'instabilité ainsi que par de fortes tensions au sein des Outre-mer (émeutes violentes en Nouvelle-Calédonie, mouvements de contestation aux Antilles), mais aussi dans le contexte de nombreuses oppositions à l'organisation de grands événements ou la réalisation de certains projets (organisation des Jeux olympiques et paralympiques, construction de l'autoroute A69, projets de bassines…), la part de la finalité tenant, entre autres, à la **prévention des violences collectives** a continué de régresser à hauteur de 11,4 % en 2024 contre 11,9 % en 2023. Le nombre de demandes invoquant cette finalité est néanmoins en très légère hausse, avec environ 300 demandes de plus que l'année précédente.

Enfin, la part de la finalité visant la défense et la promotion des intérêts économiques industriels et scientifiques majeurs s'est stabilisée à hauteur de 8,9 % en 2024, contre 9,2 % en 2023.

### Évolution du nombre de demandes par finalité les motivant entre 2020 et 2024



## Répartition des finalités fondant toutes les demandes de techniques de renseignement en 2024




- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

# Partie 2. Le contrôle de l'usage des techniques de renseignement en 2024 : de nombreux défis et un bilan contrasté

Ainsi que cela a été souligné dans les précédents rapports d'activité de la commission, le contrôle *a posteriori* exercé sur l'activité des services de renseignement répond à un triple objectif.

Il s'agit en premier lieu de comprendre le cheminement des données recueillies au moyen des techniques de renseignement et leurs conditions d'exploitation.

En deuxième lieu, il a pour objet de vérifier la régularité de l'exploitation de ces données avec un enjeu tout particulier lorsque sont concernées des professions protégées au sens des articles L. 821-7 et L. 854-3 du code de la sécurité intérieure (CSI).

Enfin, le contrôle a également une dimension informative, pédagogique et relationnelle permettant de mieux comprendre les missions et les enjeux des services de renseignement et leur transposition concrète en étant notamment au contact des opérationnels mais aussi de dissiper les éventuelles incompréhensions susceptibles de survenir.

Afin de maintenir et renforcer la crédibilité et l'efficacité de ce contrôle, la commission veille depuis plusieurs années à la sélectivité de ses contrôles et au suivi de la correction des anomalies relevées.

Cependant, ces objectifs impliquent des connaissances et des moyens en adéquation avec l'utilisation de techniques de renseignement de plus en plus intrusives, permettant la captation

d'une masse de données très hétérogènes, le recours à des systèmes de prétraitement et de traitement de ces données de plus en plus sophistiqués et la complexité et la diversité de leurs conditions de stockage.

Dans ce contexte, en 2024, la CNCTR a été confrontée à plusieurs défis pour maintenir un niveau et des modalités de contrôle efficaces et crédibles (2.1). Si comme les années précédentes, le bilan des relations avec les services à cet égard est positif, la commission déplore la persistance de certains types d'anomalies. (2.2). Par ailleurs, si le contrôle à la demande des citoyennes et des citoyens poursuit sa progression, il conduit à ce jour à très peu de contentieux devant le Conseil d'État et n'aborde les mesures de surveillance internationale que de manière marginale (2.3).

## 2.1. L'exercice du contrôle *a posteriori* en 2024 : le défi du maintien d'un contrôle efficace et crédible

### 2.1.1. La nécessaire adaptation du nombre et des modalités de contrôle dans un contexte conjoncturel exceptionnel

En 2023, les évolutions dans l'organisation et les modalités de réalisation des contrôles ainsi que le renforcement de ses effectifs avaient permis à la CNCTR de déployer une action particulièrement intense de contrôle des techniques mises en œuvre par les services, avec 136 contrôles menés sur place. **En 2024, divers motifs conjoncturels ont conduit à adapter ces contrôles tant en volume qu'en méthode**.

L'organisation des Jeux olympiques et paralympiques et une tension conjoncturelle sur les effectifs de la commission ont ainsi mené à une baisse de 9 % du nombre de contrôles réalisés, soit 123 contrôles. Cependant, il convient de relever qu'une partie de ces contrôles a été conduite selon des modalités nouvelles. Par ailleurs, dans la continuité de la stratégie développée depuis plusieurs années, les visites et contrôles dans l'hexagone et Outre-mer ont été préservés, au profit d'un dialogue constructif avec les services. Ainsi, bien qu'en deçà de ceux de l'année passée, ces chiffres traduisent une activité de contrôle *a posteriori* toujours soutenue, supérieure au nombre de contrôle mené en 2019, 2021 ou 2022[21], et plus ciblée.

### *Une inévitable diminution du nombre de déplacements dans les services dans le contexte de l'organisation des Jeux olympiques et paralympiques et de tensions conjoncturelles sur les effectifs de la commission*

Suite à des échanges préalables avec les services concernés et prenant en compte la mobilisation exceptionnelle qui leur était demandée, la CNCTR a fait le choix, sur la période s'étendant de mai à septembre 2024, d'ajuster ses déplacements dans les services, *a fortiori* les plus directement mobilisés par l'enjeu de l'organisation des Jeux olympiques et paralympiques ou d'orienter ses contrôles de façon à solliciter moins d'agents ou des agents moins directement concernés par la gestion des menaces en lien avec cet événement. Les contrôles dits de données, passant par des vérifications opérées sur les outils informatiques des services, ont été moins concernés. Cette position pragmatique de la commission, a connu des exceptions lorsque la nécessité l'imposait.

21. Une centaine de contrôles avaient été menés en 2019, 117 en 2021 et 121 en 2022 (l'année 2020 n'avait permis de réaliser que 76 dans les services dans le contexte de la crise sanitaire liée à l'épidémie de Covid-19).

Cette adaptation du volume de contrôle était nécessaire pour renforcer, sur la même période, les capacités de contrôle *a priori* de la commission afin de faire face à l'augmentation conjoncturelle du nombre de demandes de techniques soumises à des délais d'instruction contraints[22].

Enfin, **la commission a dû, de façon conjoncturelle, faire face à la fois à une baisse sensible de son effectif réel de chargés de mission** (de - 21 % à - 29 % notamment sur la période de septembre à décembre 2024) et **à son large renouvellement**.

Ces contraintes ont conduit à mener 113 contrôles directement au sein des services, auxquels doivent être ajoutés 10 contrôles approfondis à distance (voir ci-dessous), soit un total de 123 contrôles. Cette légère baisse par rapport à 2023 ne doit pas occulter l'ensemble des échanges avec les services, notamment à travers des présentations devant le collège, des interrogations concernant leur pratique ou encore des échanges avec les directions techniques, moins aisément quantifiables, mais qui contribuent substantiellement à l'exercice de la mission de contrôle *a posteriori* de la CNCTR.

### *Un maintien des contrôles dans l'hexagone et Outre-mer*

En 2024, la commission n'a pas renoncé à ses déplacements dans les centres d'exploitation du GIC situés sur l'ensemble du territoire français, y compris Outre-mer, ainsi que dans certaines entités déconcentrées des services de renseignement afin de procéder à des contrôles sur pièces et sur place approfondis[23]. Bien que lourds sur un plan logistique, ces déplacements comportent une forte dimension pédagogique à l'adresse d'entités territoriales et d'agents

22. De mai à septembre 2024, le nombre d'agents de la commission contribuant spécifiquement à la mission de contrôle *a priori* a été renforcé, notamment afin de répondre à l'augmentation du nombre de demandes adressées à la commission dans les délais prévus par le CSI, soit 24 ou 72h selon le type de demande, a été adapté de 3 à 4 personnes, puis de 3 à 5 personnes, sur un effectif total de théorique de chargés de mission de 14 personnes.

23. Voir sur ce point le 8ème rapport d'activité 2023 de la CNCTR, p. 51 et suivantes.

qui ne disposent pas toujours des mêmes ressources que les directions centrales.

Comme la commission a pu l'exposer dans ses précédents rapports, **ces déplacements** permettent notamment de **rencontrer les responsables locaux des services** et d'échanger avec eux sur l'état de la menace qu'ils doivent affronter au niveau local ainsi que sur les difficultés qu'ils constatent dans l'application du cadre légal. Dans certains cas, notamment dans les Outre-mer, ils sont également l'occasion d'entretiens avec les autorités administratives et les représentants judiciaires locaux.

Ces déplacements font l'objet d'une préparation préalable portant sur l'ensemble des suivis techniques opérés au sein de la zone par les services. En amont, les services sont également incités à faire part à la commission des thématiques qu'ils souhaitent aborder et des questions juridiques et techniques qu'ils se posent.

Au total, **la commission a ainsi réalisé onze contrôles et visites dans les territoires en 2024**, contre quinze en 2023. Ces déplacements se sont concentrés sur les centres d'exploitation du GIC dans lesquels la commission ne s'était pas déplacée depuis plusieurs années ainsi que dans les centres où les volumes de techniques actives sont plus modestes, c'est-à-dire où les services locaux mettent moins en œuvre les techniques de renseignement, afin de s'assurer que cette utilisation plus sporadique ne se fasse pas au détriment d'un strict respect du cadre légal.

### *Un accent mis sur le contrôle à distance*

Au cours de l'année 2024, s'appuyant sur ses accès directs à certaines données recueillies et aux exploitations qui en sont faites, depuis ses locaux, la commission a fortement développé le suivi à distance des productions qu'elle opère de façon quotidienne dans le cadre de sa mission de contrôle *a priori* et de la préparation de tous les contrôles sur pièces et sur place. Elle a également renforcé de façon significative le contrôle des productions issues des techniques mises en œuvre à l'encontre de professions protégées ou de communications entre une cible et une personne exerçant une profession protégée (voir point 2.1.2 du présent rapport).

Enfin, **la commission a élaboré une méthodologie spécifique**, reposant sur un cahier des charges élaboré collégialement, afin de réaliser des contrôles approfondis à distance, soit sur des thématiques transversales, soit sur des surveillances individuelles susceptibles de poser des difficultés au regard des exigences du cadre légal.

Le pôle de contrôle *a posteriori* a ainsi réalisé dix contrôles thématiques ou transversaux approfondis.

Bien qu'en pratique très chronophage, la commission dresse un premier bilan très positif de ce nouveau type de contrôle à distance qui a permis de tirer des conclusions éclairées sur différentes thématiques, voire a pu conduire à solliciter la destruction de renseignements recueillis.

## CONTRÔLER, C'EST AUSSI ACCOMPAGNER, COMMUNIQUER ET ÉCHANGER

La mission de contrôleur ne se réduit pas à la vérification du respect du cadre légal fixé par le CSI. Depuis plusieurs années, la commission poursuit une démarche d'explicitation du cadre légal et de diffusion de sa doctrine à l'attention des services. Cette démarche prend plusieurs formes.

### Les déplacements dans les services

Qu'il s'agisse de déplacements à seule fin de contrôle ou des déplacements dans les centres d'exploitation du GIC ou dans les implantations locales des services, les échanges directs avec les agents des services sont l'occasion d'expliciter certains avis rendus par la commission ainsi que, le cas échéant, des positions doctrinales retenues par le collège. Les services peuvent saisir l'occasion de ces rencontres pour porter à la connaissance de la commission des difficultés d'ordre juridique. Ces déplacements constituent un moyen de développement de connaissances réciproques des services et de la CNCTR au profit d'une meilleure application du cadre légal. Il est parfois constaté que la commission et ses missions sont encore mal connues des échelons locaux des services. Il convient donc de les expliquer et de favoriser la connaissance et le respect du cadre légal par tous les services où qu'ils soient.

### La contribution aux formations des agents des services

Depuis plusieurs années, la commission contribue très activement à la formation des agents des services de renseignement ainsi que des cadres de leurs ministères de tutelle pour développer en leur sein la connaissance du cadre juridique applicable aux techniques de renseignement en particulier à travers les formations mises en place par l'Académie du renseignement[24].

24. Sur la contribution de la commission à diverses formations, voir l'annexe au présent rapport consacrée aux relations extérieures de la commission p. 191 - 3. Les relations extérieures.

**La diffusion de la doctrine aux services**

Après avoir systématisé la compilation de sa doctrine classifiée, l'avoir consolidée puis procédé à une première diffusion à l'intention des services de renseignement relative au traitement des demandes en matière de prévention des extrémismes violents, la commission a mis en place, au début de l'année 2024, une diffusion plus régulière prenant la forme de fiches d'alerte et d'une « lettre » traitant différentes questions d'application du cadre légal examinées par le collège. La première de ces lettres, adressée aux services en mars 2024, résume et explicite les grandes évolutions de la doctrine de la commission au cours de l'année 2023 ; la seconde, transmise en octobre, est relative aux demandes portant sur les professions protégées.

### 2.1.2. Une évolution contrastée des modalités concrètes de contrôle

Si au cours de l'année 2024, plusieurs améliorations sont à noter s'agissant de l'accès de la commission à certaines informations thématiques ou techniques, les modalités de contrôle de certaines techniques demeurent aléatoires. Pour bien cerner les difficultés, un rappel des règles légales s'impose.

## Quels accès aux données pour la CNCTR ? Accès permanent, complet et direct / Accès immédiat / Accès à distance Les enjeux du contrôle

**Ce que prévoit la loi : un accès aux données par la commission moins important pour les techniques les plus attentatoires à la vie privée.**

La loi confère à la CNCTR un droit d'accès « ***permanent, direct et complet*** »[25] aux relevés de traçabilité et à l'ensemble des renseignements issus des techniques de renseignement, qu'il s'agisse des données collectées ou capitalisées (transcriptions et extractions). Lorsque les techniques visent des personnes exerçant une profession protégée, l'article L. 821-7 du code de la sécurité intérieure (CSI) prévoit, au surplus, que « *les transcriptions des renseignements collectés [...] sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats* ».

**L'accès immédiat, qui permet à la commission d'accéder, depuis ses locaux, aux données telles qu'elles sont stockées dans les systèmes d'information des services, n'est prévu que ponctuellement par la loi.** C'est le cas s'agissant des données techniques de connexion collectées en temps différé (article L.851-1 du CSI) et aux transcriptions et extractions issues des techniques d'interception de sécurité qu'elles soient émises par la voie des communications électroniques (article L. 852-1, V.), par dispositif de proximité (article L. 852-1, I.), ou par voie satellitaire (article L. 852-3). Les techniques les plus intrusives ne sont donc pas concernées.

25. L'article L. 833-2 du CSI dispose que : « *Pour l'accomplissement de ses missions, la commission : [..] 2° Dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions, extractions et transmissions mentionnés au présent livre, aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ainsi qu'aux renseignements mentionnés au III de l'article L. 822-2* ».

L'article L. 822-1 prévoit quant à lui que : « *Le Premier ministre organise la traçabilité de l'exécution des techniques autorisées en application du chapitre I du présent titre et définit les modalités de la centralisation des renseignements collectés.*

*À cet effet, un relevé de chaque mise en œuvre d'une technique de recueil de renseignement est établi. Il mentionne les dates de début et de fin de cette mise en œuvre ainsi que la nature des renseignements collectés. Ce relevé est tenu à la disposition de la commission, qui peut y accéder de manière permanente, complète et directe, quel que soit son degré d'achèvement.* »

**Dans certains cas, la loi prévoit une centralisation obligatoire des données recueillies et/ou capitalisées au sein des systèmes d'information du GIC.** C'est le cas par exemple des interceptions de sécurité émises par la voie des communications électroniques, pour lesquelles le I de l'article L. 852 du CSI prévoit un accès immédiat de la commission aux extractions et transcriptions et une centralisation obligatoire de ces opérations au sein du GIC. C'est également le cas de la technique de l'algorithme (article L. 851-3) et de la technique de la géolocalisation en temps réel (article L. 851-4[26] ).

**Les perspectives : l'accès à distance comme moyen de garantir un « accès complet et direct » aux données.**

Plus qu'un droit d'accès immédiat qui serait prévu de façon généralisée dans la loi, la CNCTR est favorable à toute perspective **d'accès à distance aux données depuis ses locaux**, dont il apparaît qu'il est, en l'absence d'accès immédiat, le seul moyen efficace de garantir qu'elle a, de façon complète et directe, accès aux données.

À titre d'illustration, lorsqu'une technique d'interception de sécurité est autorisée, la centralisation de son exécution par le GIC, chargé de transmettre les réquisitions aux opérateurs, l'exploitation des données obligatoirement réalisées sous son contrôle et l'accès à distance de la commission aux données collectées et aux productions, garantissent une visibilité exhaustive sur les conditions de mise en œuvre des techniques et d'exploitation des données recueillies. Cette configuration garantit qu'aucune donnée n'est illégalement conservée en méconnaissance d'une autorisation donnée ou ne fait l'objet d'une exploitation abusive par un service.

Lorsque la loi ne prévoit ni de centralisation obligatoire de l'exploitation de la technique au GIC, ni d'accès immédiat de la commission, comme c'est le cas notamment des techniques particulièrement intrusives de captation d'images, de paroles ou de données informatiques, deux cas de figure coexistent. Certains

26. Plus précisément, l'article L. 851-4 du CSI ne prévoit pas expressément que la technique de GTR est exécutée par le GIC, mais que les données sont transmises « à un service du Premier ministre ».

services disposent de solutions de centralisation propres tandis que les autres services disposent d'une possibilité de centralisation des données grâce à des outils offerts par le GIC.

Lorsque les techniques ne sont pas centralisées au GIC, la commission accède aux données en se déplaçant dans les locaux du service et en consultant ses systèmes d'exploitation. En vertu de son droit d'accès direct et immédiat, la CNCTR doit en principe pouvoir accéder directement à l'ensemble des extractions et transcriptions réalisées. Cependant, la commission constate régulièrement l'absence de bulletins de renseignement (ou rapports d'exploitation, c'est-à-dire des comptes rendus des informations tirées de la mise en œuvre de la technique de renseignement) relatifs à une technique pourtant présentée comme efficace par le service, l'établissement tardif de ces bulletins de renseignement, parfois plusieurs mois après l'échéance du délai de conservation des données collectées, ou la présence de données stockées sur les postes individuels de certains agents, sans traçabilité évidente, ou encore l'existence d'outils propres au service permettant une forme de capitalisation de données en dehors d'un bulletin de renseignement (voir point 2.2 du présent rapport, sur les anomalies constatées).

Ces constats interrogent sur la réalité du caractère direct et complet de l'accès de la CNCTR et renforcent la nécessité de voir se concrétiser le projet d'un accès à distance aux données issues des RDI (voir point 3.3 du présent rapport), permettant une amélioration de son accès aux données et, corrélativement, de garantir, comme elle le doit, la légalité de l'action des services au stade de l'exploitation et de la capitalisation de ces mêmes données.

### *La mise en place de dispositifs spécifiques de contrôle et l'approfondissement des connaissances techniques et thématiques*

De façon générale, afin d'améliorer ses connaissances thématiques et de mieux apprécier l'intérêt de certaines surveillances, la commission a augmenté de façon significative ses demandes aux

services de renseignement de notes thématiques ou de tout document d'information sur des cibles suivies dans le cadre de dossiers complexes, de même que ses demandes de présentations au collège, dans ses locaux ou en visioconférence sécurisée. Ces échanges présentent un avantage pour la commission aussi bien que pour les services. Du point de vue de la commission, ils permettent de mieux appréhender la démarche du service et de contextualiser ses demandes de techniques dans le cadre plus général du suivi d'une personne ou d'une thématique. Ces échanges sont également l'occasion d'alerter les services sur la fragilité juridique éventuelle de demandes qui ne seraient pas suffisamment fondées avant même qu'elles ne soient soumises. Par ailleurs, du point de vue des services, ces échanges permettent de comprendre les attentes de la commission et renforcent leur efficacité, en les mettant en situation d'éviter des avis défavorables si les demandes envisagées ne peuvent trouver de fondement légal. La commission entend poursuivre et approfondir ces échanges constructifs en 2025.

S'agissant plus particulièrement de la surveillance des professions protégées, faisant application des dispositions du 4ème alinéa de l'article L. 821-7 du CSI[27], la commission demande désormais que l'ensemble des transcriptions et extractions réalisées à partir de techniques non-centralisées (voir encadré ci-dessus) mises en œuvre à l'encontre de personnes exerçant une activité ou un mandat protégé au sens de cet article lui soit présenté à chaque contrôle.

Par ailleurs, une procédure spécifique de signalement de certaines productions relatives à ces personnes auxquelles la loi accorde une protection particulière, issues de l'exploitation des interceptions de sécurité, a été mise en place en concertation avec le GIC. Ainsi, dans des cas de figure pré-identifiés, ou à l'initiative du GIC, ce

27. Cet alinéa prévoit que « *les transcriptions des renseignements collectés en application du présent article [l'article L. 821-7 du CSI] sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats* ».

dernier transmet à la commission les projets de transcription soulevant une difficulté particulière en matière d'appréciation du caractère détachable des éléments exploités de l'activité ou du mandat protégé. Conformément à la loi, aucun élément rattachable à la profession ou au mandat ne doit en effet être conservé, ni exploité. L'avis de la commission peut conduire à la suppression de certaines productions ou au contraire permettre leur conservation, le cas échéant, après un échange approfondi avec le service.

S'agissant des connaissances techniques de la commission, des échanges réguliers avec les directions techniques de certains services du premier cercle de la communauté du renseignement se sont poursuivis au cours de l'année 2024. D'une manière générale, la commission a engagé avec plusieurs services une démarche plus globale d'appréhension des anomalies relevées lors des contrôles. Au-delà des échanges directement liés au constat et à la correction des anomalies relevées lors des contrôles menés au sein de ces services, ce dialogue technique vise à identifier de façon plus transversale les causes des irrégularités persistantes et à évoquer les ajustements et correctifs à apporter, afin de prévenir leur réitération.

### *Des modalités d'accès aux données encore imparfaites*

L'année 2024 a confirmé que l'accès de la commission aux données brutes et aux résultats d'exploitation, dans des conditions et des formats qui lui permettent de réaliser un contrôle efficace et efficient, qu'il s'agisse d'un accès, depuis ses locaux, ou, depuis les locaux des services, demeurait très aléatoire.

Si l'accès à distance de la commission aux données issues de la mise en œuvre des techniques dont l'exécution est confiée au GIC est satisfaisant et a été particulièrement investi par la commission dans le courant de l'année 2024 (voir point 2.1.1 du présent rapport), le constat reste mitigé s'agissant des autres cas de figure.

Ainsi, la commission a pu se réjouir dans ses précédents rapports de l'augmentation des solutions techniques lui permettant d'accéder depuis ses locaux aux données, transcriptions et extractions issues des techniques de captation d'images et de paroles, et plus récemment, à certaines données issues des recueils de données informatiques par les services du second cercle, ainsi qu'aux données brutes des communications mixtes interceptées dans le cadre de la surveillance internationale.

Cependant, leur utilisation aux fins de contrôle n'est pas encore pleinement efficace. En effet, trop peu déployées sur le territoire national, ou ne disposant pas d'un débit suffisant, les solutions pour la centralisation des données issues des captations d'images et de paroles sont très peu utilisées par les services. De même, l'outil de centralisation des données issues de certains RDI au GIC est très peu abondé ; les difficultés rencontrées par les services pour l'exploitation des données ne les incitant en outre pas à son utilisation (voir sur ce point la partie 3.3 du présent rapport). Enfin, la commission a, en pratique, été privée pendant plusieurs mois d'un accès effectif aux données brutes issues des communications mixtes. À ce jour, la CNCTR n'a reçu aucune explication concordante sur les motifs de cette interruption d'accès.

S'agissant par ailleurs des techniques non centralisées et dont les données ne sont accessibles que dans les locaux de certains services du premier cercle, l'accès de la commission demeure aléatoire, alors qu'il s'agit pourtant des techniques parmi les plus intrusives, au sein des services qui en mettent le plus en œuvre.

Tout d'abord, la commission rappelle que ces contrôles, qui impliquent que des agents se rendent *in situ* sur des créneaux préétablis, ont nécessairement une portée limitée sur le plan quantitatif, le nombre de techniques pouvant être effectivement contrôlées étant extrêmement réduit en comparaison au nombre de techniques autorisées.

**La commission est par ailleurs régulièrement confrontée à des difficultés d'accès aux données dans le cadre de ces contrôles**.

À titre d'illustration, s'agissant des données brutes issues de la mise en œuvre d'*IMSI catcher*, la commission a été confrontée pendant plusieurs mois à une dégradation de ses accès dans un grand service. Ainsi, alors qu'elle avait bénéficié d'un accès dans des conditions équivalentes à celles des agents exploitants, elle a été privée des outils permettant d'interpréter ces données brutes. L'accès est désormais rétabli dans des conditions satisfaisantes.

S'agissant de l'accès aux données issues des recueils de données informatiques, la commission a dû faire face à différents cas de figure mettant en évidence la dépendance de son contrôle à la disponibilité et au bon fonctionnement des outils mis à disposition par les services.

Ainsi, dans un service, une erreur dans l'attribution des droits informatiques aux agents de la commission a empêché l'accès aux données issues des RDI pendant plusieurs mois. Dans un autre service, l'obsolescence du matériel informatique mis à disposition de la commission a rendu très aléatoire l'ouverture des fichiers issus de RDI, ne permettant que rarement au contrôle d'aboutir. Dans le courant de l'été 2024, le service a procédé au changement de l'ensemble des postes informatiques dédiés au contrôle de la commission.

Si à chaque fois, les services concernés ont fait le nécessaire, une fois l'origine des difficultés identifiées, pour les résoudre, ce constat constitue un sujet de vigilance pour la commission ; l'efficacité, et par voie de conséquence, la crédibilité de son contrôle, ne sont pas structurellement acquises.

Certaines avancées annoncées n'ont pas encore abouti. À titre d'illustration, dans le cadre des échanges relatifs au projet de

centralisation de l'ensemble des techniques de recueil de données informatiques (voir rapport d'activité pour l'année 2023 et la partie 3 du présent rapport), un service du premier cercle, particulièrement concerné, s'était engagé, dans l'attente de la réalisation de ce projet, à mettre en place une procédure de communication directe à la commission d'une partie de ses transcriptions selon des modalités qui restaient à déterminer. Or, la mise en œuvre de cet engagement, qui devait intervenir postérieurement à la période des Jeux olympiques, n'est toujours pas effective. La commission veillera, avec le service, aux conditions de mise en œuvre de cette communication au cours de l'année 2025.

S'agissant du contrôle des mesures de surveillance internationale, si la commission exprime sa satisfaction de bénéficier, depuis le début de l'année 2024, d'une salle dédiée au contrôle des six services susceptibles d'y avoir recours, elle regrette de ne pas encore disposer des mêmes outils que ceux utilisés par les agents desdits services. En outre, elle est régulièrement confrontée à des difficultés logistiques : modalités d'accès aux locaux et aux données, fonctionnement du matériel mis à disposition, ergonomie et rapidité des outils de contrôle, qui nuisent à l'efficacité du contrôle et à la montée en compétence de ses agents.

## 2.2. Bilan des contrôles : des anomalies de gravité variable mais dont la persistance pose question

Le nombre des anomalies constatées en 2024 est équivalent aux années précédentes. Leur constat a donné lieu à des échanges systématiques avec les services de renseignement qui ont veillé à y mettre un terme dans des délais raisonnables, sans que la commission ait à faire usage du pouvoir de recommandation formelle que lui confère l'article L. 833-6 du CSI. La commission s'en félicite.

À titre liminaire toutefois, la commission rappelle que son activité de contrôle *a posteriori* sur les données recueillies et capitalisées par les services ne peut se faire, par hypothèse, que par échantillonnage, et ne porte, en pratique, que sur une très faible proportion de l'ensemble des données issues des techniques de renseignement mises en œuvre. Pour autant, la quasi-totalité des contrôles de données en surveillance dite domestique ou internationale donne lieu au constat d'anomalies persistantes, dont la gravité est variable, ce qui conduit la commission, après dix années d'exercice de son activité de contrôle *a posteriori*, à considérer que le nombre des anomalies effectivement constatées ne peut refléter que très partiellement la réalité.

Ce constat, a participé à ce que la commission développe, en concertation avec les services les plus concernés, une approche plus globale de l'identification des anomalies les plus récurrentes, de leurs causes et des correctifs à apporter (voir point 2.1.2 du présent rapport).

Enfin, afin de permettre une meilleure appréhension de la portée des anomalies constatées, le bilan présenté est complété cette année de deux encarts expliquant l'enjeu particulier que constitue le correct établissement des fiches de traçabilité et des bulletins de renseignements (ou rapports d'exploitation).

### 2.2.1. Les anomalies relevées au stade du recueil des données

Comme l'année précédente, des irrégularités relatives aux conditions et modalités de mise en œuvre des techniques : périmètre, durée d'autorisation, personne visée, ont été constatées. Moins fréquentes que celles liées à l'exploitation des techniques, elles présentent en revanche un degré de gravité bien supérieur

puisqu'elles conduisent au recueil de données qui n'auraient pas dû l'être, ou du moins, dans des conditions qui n'ont pas été prévues par l'autorisation donnée après avis de la commission. Toutes les irrégularités constatées ont été notifiées aux services concernés, qui ont procédé aux suppressions et correctifs demandés.

Plusieurs cas de figure « habituels » sont rencontrés.

**Certaines restrictions relatives aux modalités de mise en œuvre des techniques**, que la commission mentionne pourtant expressément dans ses avis, ne sont pas respectées. Ces restrictions visent pourtant à limiter la gravité de l'atteinte portée à la vie privée de la personne surveillée ou de tiers. En d'autres termes, elles permettent à la commission de vérifier que l'atteinte portée à la vie privée est bien proportionnée à la menace que chaque personne représente. Les manquements de nouveau constatés en 2024 ont concerné, comme l'année précédente, la technique de recueil de données informatiques qui recouvre des modalités de mise en œuvre très différentes dont l'intrusivité varie grandement. Le service concerné a fait évoluer sa pratique et ses outils afin que les restrictions apportées par la commission soient effectivement prises en compte.

La commission appelle à cet égard les services à une vigilance particulière s'agissant de la prise en compte de ses avis comportant des restrictions.

**Des données ont été recueillies alors que l'autorisation de mise en œuvre était arrivée** à échéance. Dans un cas, cette mise en œuvre d'une technique au cours d'une période appelée « de carence » est apparue d'autant plus problématique que la fiche de traçabilité renseignée par le service était erronée puisqu'elle faisait état d'une désactivation du dispositif techniques de recueil. Le contrôle a toutefois permis de conclure à l'absence de mauvaise foi du service. Les données ont été détruites et la traçabilité modifiée à

la demande de la commission. L'attention des services doit toutefois être attirée sur la nécessité de se doter d'un dispositif interne, d'abord organisationnel et si possible technique, visant à garantir que l'échéance d'une autorisation de mise en œuvre soit systématiquement respectée, cela par tous les échelons impliqués dans la mise en œuvre de la technique.

**Des anomalies tenant au dépassement de l'objet de la surveillance** ont de nouveau été constatées. Il s'agit d'hypothèses dans lesquelles un service continue à mettre en œuvre une technique alors que la personne surveillée n'est pas ou plus présente dans le lieu spécifiquement visé dans l'autorisation. Elles résultent en général d'une difficulté à paramétrer le dispositif de captation et de contraintes opérationnelles liées à la nature spécifique de certains lieux qui ne permettent pas aux agents d'intervenir immédiatement afin de limiter la mise en œuvre au strict nécessaire. La commission invite l'ensemble des services pouvant être concernés à mettre en place une procédure interne de détection et de suppression des données ainsi indûment collectées qui soit la plus rapide possible.

Deux cas de figure plus atypiques peuvent également être évoqués.

**Le premier concernait un usage particulièrement atypique de la technique de captation d'images dans un lieu privé**. Le service, qui considérait que ce dernier ne relevait pas des dispositions de l'article L. 853-1 du CSI, n'avait pas demandé d'autorisation de mise en œuvre. La commission a néanmoins considéré que les techniques mises en œuvre auraient bien dû faire l'objet d'une autorisation sur le fondement des articles L. 853-2 et L. 853-3 du CSI et l'a notifié au service qui a indiqué avoir retiré le matériel et supprimé les données collectées.

**Le second a mis en lumière une carence d'un service dans la réalisation des vérifications nécessaires à la détection de l'exercice par la personne surveillée d'une profession protégée.**

L'hypothèse de la découverte fortuite, en cours d'exploitation d'une technique, de l'exercice par la personne concernée d'un mandat ou d'une profession protégé a déjà été rencontrée et ne constitue pas, en tant que telle, une irrégularité. Si elle ne peut tout à fait être exclue, les services ont en revanche la responsabilité de réaliser les investigations nécessaires pour prévenir autant que possible ce cas de figure. Dans le cas d'espèce, le service avait sollicité des autorisations de mise en œuvre de techniques de renseignement à l'égard de personnes dont l'identité, et donc la profession, étaient encore inconnues au moment du traitement de la demande. Il avait toutefois garanti qu'il procéderait aux vérifications permettant les identifications dès que possible et, en tout état de cause, avant la mise en œuvre des techniques. La commission, qui a constaté que ces vérifications n'avaient pas été réalisées lorsque le service l'a, de sa propre initiative, informée de la découverte de la profession exercée par les personnes visées, a demandé la destruction des données. Ces irrégularités ont également fait l'objet d'un courrier du président de la CNCTR au directeur du service.

### 2.2.2. Les anomalies constatées en matière de traçabilité de la mise en œuvre des techniques de renseignement

Des carences récurrentes dans l'établissement et la transmission des relevés de mise en œuvre, appelés « fiches de traçabilité » ont de nouveau été notées en 2024.

**Sans traçabilité correcte, la commission ignore si une technique autorisée a effectivement été mise en œuvre et dans quelles**

**conditions**. Cela limite sa capacité à préparer efficacement les contrôles *a posteriori*, mais surtout à détecter les éventuelles anomalies et, le cas échéant, à instruire de façon éclairée les demandes de renouvellement des techniques concernées. La commission encourage ainsi régulièrement les services à faire preuve de rigueur dans l'établissement des fiches de traçabilité, même lorsque la technique n'a pas été mise en œuvre.

En outre, à deux reprises en 2024, des démarches plus spécifiques ont été engagées sur ce sujet. D'une part, à l'attention d'un service pour lequel la commission avait constaté à de nombreuses reprises que les fiches de traçabilité n'étaient pas renseignées ou très tardivement, ou encore qu'elles n'étaient pas suffisamment précises, alors qu'il avait réalisé des efforts notables sur le sujet les années précédentes. Des engagements ont été pris pour une amélioration des pratiques mais devront être vérifiés au cours de l'année 2025. D'autre part, il s'agissait pour un service de renseigner de façon plus détaillée la traçabilité de la mise en œuvre des techniques de sonorisation, qui impliquaient la mise en place de plusieurs dispositifs techniques, et de recueil de données informatiques. Le service concerné a rapidement procédé aux évolutions demandées.

## À QUOI SERT UNE FICHE DE TRAÇABILITÉ ?

Aux termes de l'article L. 822-1 du code de la sécurité intérieure (CSI), un relevé de mise en œuvre de chaque technique de renseignement, mentionnant « *les dates de début et de fin de mise en œuvre ainsi que la nature des renseignements collectés* », *doit être établi. Ce relevé, plus couramment désigné sous le terme de « fiche de traçabilité* », est « *tenu à la disposition de la commission qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement* ».

Le 2° de l'article L. 833-2 du CSI prévoit quant à lui que la commission « *dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions, extractions et transmissions mentionnés au présent livre, aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ainsi qu'aux renseignements mentionnés au III de l'article L. 822-1* ».

En pratique, les fiches de traçabilité sont transmises à la commission par le biais de l'outil de demande et de validation des techniques de renseignement mis à disposition par le GIC et auquel les services, la commission et le Premier ministre ont accès depuis leurs locaux respectifs. La commission peut également les consulter directement dans les systèmes d'information des services lors de ses déplacements dans leurs locaux.

Leur renseignement complet et rapide est primordial afin de permettre aux différents acteurs du contrôle de la légalité de la mise en œuvre des techniques de renseignement, y compris ceux du contrôle interne, de procéder aux vérifications nécessaires à leurs missions respectives.

Elles permettent tout d'abord au service lui-même de vérifier que les conditions de mise en œuvre respectent le cadre légal et celui de l'autorisation. La rédaction de la fiche de traçabilité et le contrôle hiérarchique réalisé au moment de sa validation sont en effet autant

d'étapes qui sont censées permettre à l'agent et à sa hiérarchie de constater qu'une irrégularité a été commise au cours de la mise en œuvre d'une technique.

Le GIC procède ensuite à un contrôle des fiches de traçabilité qui consiste à vérifier l'effectivité de leur transmission par les services et à détecter les incohérences entre les éléments portés dans la demande d'autorisation et ceux présents dans la fiche. Lorsqu'il détecte une anomalie, il la notifie au service et, en l'absence de réponse, peut en rendre compte au Premier ministre qui peut décider d'interrompre la technique.

Les fiches de traçabilité permettent enfin à la CNCTR d'accéder aux informations nécessaires, d'une part, pour instruire de façon éclairée les demandes de renouvellement, et d'autre part, pour détecter des irrégularités avant même d'accéder aux données, ou en tout cas d'identifier les éléments nécessaires à la préparation de ses contrôles.

### 2.2.3. Les anomalies relevées en matière de conservation et d'exploitation des données

Le caractère récurrent, voire structurel s'agissant de certaines techniques de renseignement, des anomalies liées à la conservation et à l'exploitation des données est régulièrement évoqué par la commission dans ses rapports d'activité. Leur persistance doit être déplorée près de dix ans après la loi du 24 juillet 2015.

**Il s'agit en premier lieu de cas de dépassement de la durée légale de conservation des données collectées**[28]. Plus nombreuses qu'en 2023, ces irrégularités ont concerné des données provenant, en majorité, des techniques les plus intrusives, en l'occurrence de captation de paroles et de recueil de données informatiques.

28. Ces durées sont fixées par les dispositions du I de l'article L. 822-2 du CSI.

Or, ces cas de figure ont principalement été rencontrés au sein d'un service du premier cercle recourant à un dispositif de centralisation propre des données. Dans cette hypothèse, les données échappent au mécanisme de centralisation organisé par le GIC (voir l'encadré consacré aux différentes modalités d'accès aux données pour la CNCTR p. 66). Comme rappelé dans le rapport d'activité pour l'année 2023, il en résulte que le respect des règles de conservation et d'exploitation des données collectées repose sur la fiabilité des procédures internes mises en place par les services.

Dans la majorité des cas, les irrégularités étaient dues à une défaillance du script d'effacement automatique des données mis en place par le service, ayant conduit à une conservation trop longue des données brutes recueillies. Les échanges avec le service concerné ont permis d'identifier la difficulté et l'ont conduit à procéder aux développements informatiques destinés à résoudre le problème qui était à l'origine d'irrégularités récurrentes. Les données ont par ailleurs immédiatement été détruites par ce service.

**S'agissant de l'exploitation des données, la commission procède au contrôle des « extractions » et « transcriptions »** qui constituent des données que le service estime « pertinentes » et qui, à ce titre, peuvent être conservées tant qu'elles demeurent « ***indispensables à la poursuite des finalités*** » légales[29]. Comme chaque année, la commission a constaté plusieurs cas de transcription[30] portant sur des éléments sans lien évident avec la finalité poursuivie, voire avec la personne concernée par la technique. D'autres cas ont porté sur la retranscription d'éléments non détachables de l'activité protégée[31] exercée par la personne surveillée ou son interlocuteur. Ce type d'irrégularités qui peuvent

29. Voir le III de l'article L. 822-3 du CSI.

30. Ces transcriptions sont capitalisées dans des bulletins de renseignement.

31. Au sens des dispositions de l'article L. 821-7 du CSI.

être qualifiées de « classiques » conduit à un échange avec le service qui peut faire état d'éléments pertinents permettant *in fine* de justifier d'un lien avec la finalité ou la cible et, par conséquent, de fonder la conservation des informations. À défaut, elles sont détruites par le service qui doit en justifier auprès de la commission.

**Enfin et surtout, c'est de nouveau l'absence pure et simple de bulletins de renseignement (ou « résultats d'exploitation ») qui a, de nouveau, attiré l'attention de la commission en 2024**[32]. Ces manquements sont récurrents, notamment lorsque l'exploitation des techniques n'est pas centralisée au GIC. Ils font l'objet de rappels réguliers de la part de la commission car ils sont particulièrement problématiques.

En effet, sans établissement d'un bulletin de renseignement ou lorsqu'il ne comporte pas certaines mentions minimales, le contrôle de la commission est rendu très difficile. Or, les anomalies constatées en la matière concernent le plus souvent les techniques les plus intrusives, en raison de la moindre centralisation de leur exécution et d'un accès plus limité de la commission aux données.

La persistance des manquements liés, selon les cas, à l'incomplétude, à l'absence, ou au retard dans la mise à disposition des résultats d'exploitation, déjà constatés les années précédentes, a conduit le président de la CNCTR à échanger de façon plus formelle avec la direction d'un service. Celle-ci s'est engagée à procéder aux rappels nécessaires à l'égard de ses agents et à prendre des dispositions internes, en ce qui concerne le caractère complet des bulletins de renseignement, leur délai d'établissement et leur réalisation dans les outils dédiés à l'exploitation, dans des conditions permettant un accès direct et complet de la CNCTR. Les contrôles réalisés en 2025 permettront de déterminer si les améliorations annoncées sont effectives.

32. Voir encadré ci-dessous.

## LES CARENCES EN MATIÈRE DE BULLETINS DE RENSEIGNEMENT : CONTRÔLE DE LA COMMISSION, PROBLÉMATIQUES CONCRÈTES ET ENJEUX

Les « bulletins de renseignements », autrement appelés « rapports d'exploitation », « résultats d'exploitation » ou encore « productions » correspondent aux « ***renseignements extraits ou transcrits*** » dont l'objet, la conservation, la transmission et la destruction sont régis par les dispositions des articles L. 822-3 et L. 822-4 du code de la sécurité intérieure (CSI). Le I de l'article L. 822-3 prévoit ainsi notamment que « ***les renseignements ne peuvent être collectés, transcrits, extraits ou transmis pour d'autres finalités que celles mentionnées à l'article L. 811-3*** ». Le III du même article dispose quant à lui que « ***les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées au I*** ».

La loi définit donc ces renseignements « extraits ou transcrits » par leur objet. **Il s'agit en pratique des informations « pertinentes » au regard des finalités mentionnées à l'article L. 811-3 du CSI.** Ce lien avec une ou plusieurs finalités légales justifie la conservation de ces renseignements par le service au-delà du délai de conservation légale des données collectées, tant qu'ils demeurent indispensables à la poursuite desdites finalités. On parle alors de données « capitalisées ».

**Les acteurs du contrôle**

L'exploitation des techniques de renseignement est tout d'abord soumise à un contrôle interne aux services qui a pour fonction d'assurer le respect du cadre légal par les agents.

Le GIC réalise quant à lui un contrôle exhaustif de l'ensemble des productions (transcriptions ou extractions) réalisées par les services s'agissant des techniques de renseignement dont il centralise l'exploitation. Chaque projet de transcription ou d'extraction donne ainsi lieu à une vérification de la traçabilité de la mise en œuvre de la

technique concernée, du lien entre les éléments exploités et l'objectif désigné dans l'autorisation ainsi que du rapport entre ces éléments et la ou les finalités de l'article L. 811-3 du CSI invoquées. S'agissant des personnes exerçant une profession ou un mandat protégé, le GIC s'assure également que les renseignements exploités sont bien détachables de l'activité protégée. Seules les productions validées par le GIC sont ensuite transmises aux services.

Lorsque l'exploitation a lieu en dehors des systèmes d'information du GIC, ce contrôle peut être réalisé sur pièces et sur place, le GIC disposant des mêmes accès que la CNCTR aux données collectées, aux dispositifs de traçabilité et aux résultats d'exploitation.

La CNCTR dispose depuis ses locaux d'un accès à l'ensemble des productions validées par le GIC s'agissant des techniques dites « centralisées ». Pour les autres, la commission se déplace dans les locaux des services de renseignement pour procéder à leur contrôle.

**L'objet du contrôle de la commission**

Les opérations de retranscription sont soumises au contrôle de la CNCTR.

L'article L. 833-2 du CSI prévoit ainsi notamment que « *pour l'accomplissement de ses missions, la commission : […] 2° Dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions, extractions et transmissions mentionnés au présent livre, aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ainsi qu'aux renseignements mentionnés au III de l'article L. 822-2* ».

Lorsque ces opérations portent sur des renseignements visant des personnes exerçant une profession protégée, l'article L. 821-7 du CSI prévoit en outre que « *les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats* ».

Enfin, en vertu de l'article L. 833-6 du CSI, « *la commission peut adresser, à tout moment, au Premier ministre, au ministre responsable de son exécution et au service concerné une recommandation tendant à ce que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits lorsqu'elle estime que : […] 3° La collecte, la transcription, l'extraction, la conservation, la destruction des renseignements collectés ou leur transmission entre services est effectuée en méconnaissance du chapitre II du titre II du présent livre.* »

**La loi régit ainsi principalement les missions de la commission, s'agissant des renseignements « extraits ou transcrits », sous l'angle des modalités d'accès dont elle dispose auxdits renseignements et de ses pouvoirs de recommandation en la matière, sans définir précisément l'objet de son contrôle.** En effet, l'article L. 833-6 du CSI renvoie, dans des termes très généraux, à la « méconnaissance » des règles de procédure relatives à la mise en œuvre des techniques de renseignement. L'objet du contrôle exercé par la commission est donc vaste.

En pratique, le contrôle des bulletins de renseignement a un triple objet.

La CNCTR s'assure tout d'abord que les services procèdent bien à l'établissement de ces bulletins de renseignement et qu'elle y ait un accès direct. Plus précisément, elle contrôle que les éléments que les services capitalisent ne le sont pas sur des supports auxquels elle n'aurait pas un accès direct, en méconnaissance des dispositions prévues par l'article L. 833-2 du CSI. Elle s'interroge ainsi régulièrement sur l'absence de bulletins de renseignement, alors que la technique est qualifiée de productive par le service lorsqu'il sollicite le renouvellement de l'autorisation de la mettre en œuvre. Cette absence révèle que, s'agissant des techniques non « centralisées » au GIC et malgré le développement de systèmes d'information dédiés à l'exploitation des données, la pratique de certains agents consistant à travailler sur des fichiers propres non centralisés, sans aucune traçabilité et, par conséquent, aucun contrôle possible est encore fréquente.

Lorsqu'un bulletin de renseignement a été rédigé, la commission procède au contrôle de la pertinence des informations qu'il contient et qui fonde leur conservation par le service : les renseignements capitalisés sont-ils pertinents au regard de l'objet de la surveillance ? Portent-ils sur la personne visée par l'autorisation ? Les éléments sont-ils bien détachables de la profession ou du mandat protégé exercé par celle-ci ?

Enfin, les bulletins de renseignement contiennent un certain nombre d'éléments, en plus du renseignement issu de l'exploitation, qui permettent d'éclairer la commission sur la régularité et la légalité de la mise en œuvre de la technique. Le nombre très limité d'éléments pertinents retranscrits par le service peut, par exemple, conduire la commission à s'interroger sur la poursuite de la surveillance alors qu'elle ne paraît pas produire de renseignement utile, tout en portant une atteinte réelle à la vie privée de la personne concernée. La CNCTR peut également être conduite à questionner le choix de la finalité au titre de laquelle l'autorisation a été accordée. Elle peut encore détecter des anomalies liées à la mise en œuvre irrégulière de la technique, par exemple quant au lieu réel de mise en œuvre de la technique ou à la personne censée être visée par la technique.

À cet égard, la commission insiste régulièrement sur la nécessité de bien rédiger les bulletins de renseignement, s'agissant des techniques « non centralisées », sans quoi les services ne la mettent pas en mesure de procéder à son contrôle du respect du cadre légal. Un certain nombre d'informations doivent nécessairement apparaître, notamment celles permettant de caractériser la présence de la personne visée lorsqu'il s'agit d'exploiter ses conversations ou les images qui ont pu être captées, de déterminer la date de recueil de données qui font l'objet de l'exploitation ou encore les modalités de recueil et les supports éventuellement concernés. Elle invite les services à s'inspirer autant que possible du modèle de résultats d'exploitation présents dans les outils du GIC pour les techniques « centralisées ».

### 2.2.4. Les anomalies constatées en matière de surveillance des communications électroniques internationales[33]

En la matière, comme les années précédentes, la commission a constaté des anomalies récurrentes consistant en l'exploitation voire la capitalisation de communications nationales.

#### *Les anomalies liées à des surveillances touchant le territoire national*

En 2024, les contrôles ont révélé à plusieurs reprises, dans différents services, la capitalisation de données de connexion collectées à propos d'une personne surveillée alors que celle-ci se trouvait sur le territoire national ou y résidait possiblement, sur le fondement d'une autorisation d'exploitation du dispositif de surveillance internationale et ce, tant en l'absence de techniques individualisées autorisées sur cette personne qu'en dehors des régimes spécifiques autorisant une éventuelle capitalisation de données dans cette situation.

Ce type d'anomalie a pu être constaté dans des fichiers contenant des données de connexions révélant des communications localisées sur le territoire national. S'agissant des contenus, la CNCTR a découvert à plusieurs reprises dans des bulletins de renseignement synthétisant les informations recueillies au moyen d'une autorisation d'exploitation, la capitalisation d'informations successives alors que la présence ou la résidence de la personne surveillée sur le territoire national était apparente.

Ces constats ont pu être expliqués par les services concernés comme provenant d'erreurs de la part des agents exploitants et découlant d'une maîtrise insuffisante du cadre légal, associées à une difficulté de contrôle systématique de la masse de données

33. Voir encadré de présentation du cadre juridique de la surveillance internationale en p. 50 du présent rapport.

capitalisées au moyen des différentes autorisations d'exploitation relatives aux communications internationales.

Dans ces différentes situations, la CNCTR a contrôlé que ses demandes de destruction des données qui n'auraient pas dû être capitalisées avaient bien été exécutées.

### *Les anomalies portant sur des professions protégées au sens de l'article L. 854-3 du CSI*

Certaines anomalies, plus rares, ont trait à la découverte, lors d'un contrôle *a posteriori*, de l'exercice d'une profession ou d'un mandat protégé par une personne ayant fait l'objet d'une capitalisation de données au titre de la surveillance internationale alors que celle-ci exerce sur le territoire national. Dans ces cas, la CNCTR demande au service de présenter une nouvelle demande d'autorisation d'exploitation des données de connexions ou de contenus, selon le besoin, soumise au collège dans sa formation plénière, comme l'exige la loi, afin que soit examiné le caractère détachable des éléments recherchés de la profession ou du mandat protégé.

### *Les anomalies relatives au type de données faisant l'objet de requêtes des agents*

D'autres anomalies, constatées à plusieurs reprises, sont relatives au type de données ayant fait l'objet d'une recherche et d'une capitalisation par le service alors que l'autorisation d'exploitation accordée ne correspond pas au type de données qui peuvent être recherchées ou capitalisées sur son fondement.

Par ailleurs, les services accèdent parfois à des données de connexion qui les intéressent alors qu'ils n'ont pas explicitement mentionné ces données dans les documents joints à la demande d'autorisation comme l'exige le cadre légal. Dans le cas d'un grand nombre de données de connexion pour une personne visée, les services ont pu omettre d'effectuer ce travail de référencement en

amont de leurs recherches, ce qui amène à un contrôle plus long et fastidieux de vérification de l'origine et de la raison qui motive la recherche de cette donnée.

Ces différents types d'anomalies peuvent s'expliquer par des erreurs de compréhension et par suite, d'application, du champ des autorisations accordées concernant la nature de données auxquelles il est permis d'accéder ainsi que de l'étendue et de la précision des informations qu'elles matérialisent pour le service.

Au cours de l'année 2024, le travail de caractérisation technique des données concernées, d'explicitation du champ d'application des différentes autorisations prévues aux articles L. 854- 1 et suivants du CSI et de clarification et de diffusion de la doctrine de la commission, initié au cours des années précédentes, s'est poursuivi en lien avec les services de renseignement afin d'éviter la survenue de ce type d'anomalies.

### *Les anomalies liées à une absence de lien avec des composants constitutifs nécessaires de l'autorisation d'exploitation*

La CNCTR est régulièrement amenée à constater lors de ses contrôles un lien parfois ténu, voire absent, entre les éléments recueillis au moyen d'une autorisation d'exploitation et capitalisés dans des bulletins de renseignement, et la finalité ou les finalités mentionnées à l'article L. 811-3 du CSI sur le fondement desquelles l'autorisation d'exploitation a été accordée.

Il peut s'agir une absence de lien avec la zone géographique couverte par l'autorisation, ou encore d'une recherche sur une entité qui, n'avait pas été mentionnée dans la ou les listes associées à une autorisation, ou bien dont le lien apparaît insuffisant avec la finalité sur le fondement de laquelle l'autorisation a été délivrée.

La CNCTR veille à rappeler aux services la nécessité d'observer une démarche rigoureuse et d'apporter un soin particulier à la

cohérence des différentes mentions composant une autorisation d'exploitation tout au long de son cycle de vie, tant dans sa formalisation légale, que dans les résultats qu'elle permet d'obtenir.

### *Les anomalies liées à la période d'exploitation autorisée*

Les contrôles de l'utilisation des autorisations d'exploitation mettent parfois en évidence l'existence de collecte de renseignements pendant des périodes dites de carence, intervenant faute de démarche de renouvellement de l'autorisation concernée avant l'échéance de la période d'autorisation. Il peut aussi être ponctuellement observé quelques dépassements de durée d'autorisation dans le cas de régime d'utilisation spécifique et/ou d'une justification peu rigoureuse des différentes périodes de temps d'exploitation autorisées conduisant la CNCTR à solliciter l'effacement des données recueillies en dehors de la période autorisée.

## 2.2.5. Les suites apportées aux constats d'anomalies

Tout comme en 2023, tous les constats et analyses dressés par la commission au cours de l'année 2024 ont fait l'objet d'un consensus avec les services de renseignement qui ont veillé à mettre un terme aux anomalies constatées dans des délais raisonnables, sans que la commission ait à faire usage du pouvoir de recommandation formelle que lui confère l'article L. 833-6 du CSI ou à rendre un avis défavorable au renouvellement de l'autorisation de mise en œuvre concernée par l'irrégularité.

Cette année, la commission n'a, par ailleurs, **pas eu à constater d'erreur dans les procès-verbaux adressés par les services à la suite de demandes de destruction de données collectées ou de transcriptions**. Elle se félicite de ce progrès.

Les manquements persistants ou récurrents, appelant une intervention hiérarchique et l'implication continue des entités de contrôle interne des services, peuvent conduire à un signalement plus formel par le président de la commission au directeur du service concerné. **La commission reste très attentive aux résultats des démarches engagées ou annoncées par le service concerné**.

## 2.3. Le contrôle à l'initiative des particuliers : des réclamations qui continuent à augmenter sans conduire à un contentieux plus nourri devant le Conseil d'État et sans interroger les mesures de surveillance internationale

La CNCTR peut être saisie par toute personne qui souhaite vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Cette procédure de réclamation préalable est prévue par les dispositions de l'article L. 833-4 du CSI en ce qui concerne les techniques dites domestiques et par celles de l'article L. 854-9 du même code, en ce qui concerne la surveillance des communications électroniques internationales.

Le pouvoir de vérification ainsi confié à la commission porte sur les seules techniques de renseignement prévues par le CSI et ne s'étend donc ni aux mesures de surveillance ordonnées par l'autorité judiciaire ni à celles, bien entendu illégales, que pratiqueraient des personnes privées.

Pour des motifs de sécurité nationale, et en application des dispositions du décret n° 2015-1405 du 5 novembre 2015 relatif aux exceptions à l'application du droit des usagers de saisir l'administration par voie électronique, les personnes qui souhaitent que des

vérifications soient menées les concernant ne peuvent valablement saisir la commission que par lettre envoyée par voie postale.

La réclamation doit être présentée par la personne concernée ou son représentant légal, justifiant de son identité, et mentionner les identifiants techniques à partir desquels elle souhaite que les vérifications soient conduites. Ces éléments techniques, notamment des numéros de téléphone ou des adresses de messagerie électronique, doivent être assortis de justificatifs, tels qu'un contrat d'abonnement ou une facture.

Les vérifications ne peuvent avoir lieu que lorsque l'ensemble de ces informations et justificatifs a été communiqué à la commission. Les réclamations complètes sont ensuite instruites de la même manière et en utilisant les mêmes outils que lorsque la commission effectue de sa propre initiative un contrôle *a posteriori*.

### 2.3.1. Une progression continue de la quantité comme de la précision des réclamations

Si l'année 2023 avait permis de constater une hausse importante du nombre de réclamations, avec une progression annuelle de plus de 65 %, cette croissance s'est fortement ralentie en 2024. Avec 87 réclamations reçues en 2024 contre 81 en 2023, l'augmentation est de 7,5 %.

| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|---|
| **Nombre de réclamations** | **49** | **54** | **30** | **47** | **33** | **48** | **49** | **81** | **87** |

L'année 2024 a confirmé une tendance déjà relevée lors du précédent rapport d'activité s'agissant du caractère complet des dossiers de réclamations reçues.

En effet, la proportion de demandes en état d'être instruites à réception, et donc sans solliciter du réclamant l'envoi de pièces complémentaires, est en constante progression, passant de 18,4% en 2022 à 34,4% en 2023 et à 44,8% en 2024.

En outre, 9 des réclamations reçues en 2024 soit un peu plus de 10 %, sont le fait de réclamants ayant déjà sollicité la CNCTR aux fins de vérifications durant les années précédentes, ou, pour l'une d'entre elles, durant cette même année 2024.

L'ensemble de ces éléments atteste de la part du public une meilleure connaissance de l'existence et des modalités de saisine de la CNCTR.

Comme les années précédentes, le délai de réponse aux réclamations contenant toutes les informations nécessaires à leur traitement a été nettement inférieur à deux mois[34].

Aucune réclamation n'a conduit la CNCTR à adresser de recommandation au chef du service de renseignement concerné, au ministre dont il relève ou au Premier ministre pour que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits, conformément à l'article L. 833-6 du CSI.

### 2.3.2. Les recours devant le Conseil d'État restent très peu nombreux

Les articles L. 773-1 et suivants du code de justice administrative prévoient une procédure contentieuse spéciale permettant de demander à une formation spécialisée du Conseil d'État de vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à l'encontre d'une personne. Les

34. Ce délai court à compter de la date à laquelle la réclamation est en état d'être instruite. Lorsqu'une demande de pièces complémentaires (justificatifs d'identité, justificatifs d'abonnement…) a été adressée à l'auteur de la réclamation, ce délai ne commence à courir qu'à compter de la réception de ces pièces.

membres et le rapporteur public de la formation spécialisée sont habilités ès qualités à connaître d'informations couvertes par le secret de la défense nationale.

S'agissant des techniques de renseignement relevant de la surveillance domestique, la formation spécialisée du Conseil d'État peut être saisie, sur le fondement de l'article L. 841-1 du CSI, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR.

S'agissant des mesures de surveillance des communications électroniques internationales, seuls le président ou trois membres au moins de la commission peuvent saisir le Conseil d'État. Le régime de la surveillance domestique s'applique toutefois si la vérification porte sur la légalité de l'exploitation de communications de personnes utilisant des identifiants rattachables au territoire national et communiquant depuis ou vers la France. Ces personnes peuvent saisir elles-mêmes le Conseil d'État après réclamation préalable auprès de la commission[35].

**Sept nouvelles requêtes ont été enregistrées devant le Conseil d'État sur le fondement de l'article L. 841-1 du CSI en 2024**, contre cinq l'année précédente, et neuf décisions ont été rendues, dont quatre concernaient des affaires enregistrées en 2023. Au 31 décembre 2024, deux affaires enregistrées en 2024 demeuraient en instance.

La CNCTR est informée de toute requête introduite sur le fondement de l'article L. 841-1 du CSI et est invitée à présenter, le cas échéant, des observations écrites ou orales. Elle a, ainsi, le statut d'observateur devant le Conseil d'État. En tant qu'autorité décisionnaire, le Premier ministre, représenté par le GIC, a qualité pour défendre au nom de l'État.

35. Voir ci-dessous point 2.3.3.

La CNCTR a produit des observations sur toutes les requêtes qui lui ont été communiquées par le Conseil d'État.

Comme les années précédentes, la commission ne s'est pas trouvée dans la situation d'exercer elle-même un recours contentieux devant le Conseil d'État sur le fondement de l'article L. 833-8 CSI. Cette voie de recours est ouverte au président de la commission ou à trois de ses membres lorsque le Premier ministre ne donne pas suite, ou insuffisamment suite, aux avis ou aux recommandations de la commission[36].

### 2.3.3. Une absence de saisine directe en matière de surveillance internationale tandis que les modalités de contrôle en la matière n'ont pas connu d'amélioration

En vertu des dispositions de l'article L. 854-9 du CSI, toute personne qui souhaite vérifier qu'aucune mesure de surveillance des communications électroniques internationales ou de vérification ponctuelle[37] n'est ou n'a été irrégulièrement mise en œuvre à son égard peut saisir la CNCTR d'une demande en ce sens.

36. La commission n'a pas davantage été conduite à saisir le Conseil d'État d'une requête présentée dans les conditions prévues par les dispositions du deuxième alinéa de l'article L. 821 1 du CSI tel qu'il a été modifié par la loi du 30 juillet 2021. En application de ces dispositions, le président de la CNCTR ou l'un de ses membres ayant la qualité de magistrat, doit immédiatement saisir le Conseil d'État lorsque le Premier ministre délivre une autorisation de mise en œuvre d'une technique de renseignement après avis défavorable de la commission. Le Conseil d'État statue alors dans un délai de vingt-quatre heures à compter de cette saisine. La décision d'autorisation du Premier ministre ne peut être exécutée avant que le Conseil d'État ait statué, sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné sa mise en œuvre immédiate. En 2023, comme les années précédentes, le Premier ministre a suivi tous les avis défavorables émis par la CNCTR.

37. L'autorisation du Premier ministre d'exploiter les communications émises ou reçues à l'étranger ou les seules données de connexion interceptées vaut autorisation d'effectuer au sein des données de connexion interceptées des vérifications ponctuelles aux seules fins de détecter une menace pour les intérêts fondamentaux de la Nation liée aux relations entre des numéros d'abonnement ou des identifiants techniques rattachables au territoire français et des zones géographiques, organisations ou personnes mentionnés au 3° du III de l'article L. 854-2 du CSI. À la seule fin de détecter, de manière urgente, une menace terroriste, cette vérification ponctuelle peut porter sur les communications de numéros d'abonnement ou d'identifiants techniques rattachables au territoire national. Des vérifications ponctuelles peuvent également être mises en œuvre pour détecter sur les communications d'identifiants techniques rattachables au territoire national, à des fins d'analyse technique, des éléments de cyberattaques susceptibles de porter atteinte aux intérêts fondamentaux de la Nation.

Comme en matière de surveillance domestique, la commission s'assure alors que les mesures de surveillance éventuellement mises en œuvre respectent le cadre légal et réglementaire applicable ainsi que les décisions et autorisations du Premier ministre. Aux termes des vérifications menées, elle notifie à l'auteur de la réclamation qu'il a été procédé à ces vérifications, sans confirmer ni infirmer la mise en œuvre de mesures de surveillance ou de vérification ponctuelle.

En 2024, une réclamation a été regardée comme portant sur la vérification de la régularité de la mise en œuvre de mesures de surveillance internationale. En effet, lorsque les éléments portés à sa connaissance dans la réclamation comportent un élément d'extranéité : identifiants étrangers, liens avec un autre État, la commission procède d'office à des vérifications en la matière.

Cependant, dans la continuité des observations formulées par la commission dans son précédent rapport d'activité[38], il y a lieu de souligner que si les réclamations dont elle est saisie devaient plus fréquemment porter sur les mesures de surveillance internationale ou comporter des éléments la conduisant à procéder d'office à des vérifications, les modalités concrètes de son contrôle en la matière rendraient très délicat le respect du délai de deux mois au terme duquel le réclamant peut saisir le Conseil d'État.

En effet, l'absence d'accès à distance aux applications informatiques utilisées par les services en la matière impose de mener un contrôle dans chacun des six services spécialisés de renseignement pouvant avoir recours aux mesures de surveillance des communications électroniques internationales afin de procéder aux vérifications nécessaires, qui peuvent être longues et complexes.

38. Voir le 8ème rapport d'activité 2023 de la CNCTR, p. 58 et suivantes.

# Partie 3. Les sujets de vigilance et les perspectives pour l'année 2025

## 3.1. La décision du 10 décembre 2024 de la Cour européenne des droits de l'homme sur les requêtes visant le dispositif législatif français en matière de renseignement consacre le rôle de la CNCTR mais laisse plusieurs sujets de fond en suspens

Ainsi que le rappelait la commission dans son précédent rapport[39], la Cour européenne des droits de l'homme a été saisie en 2015 de douze requêtes émanant de journalistes, d'avocats et d'organismes représentant les intérêts de ces professions, puis en 2017 de deux requêtes supplémentaires émanant de journalistes. L'ensemble des requérants soutenaient que la législation française en matière de techniques de renseignement, résultant de la loi n° 2015-912 du 24 juillet 2015, méconnaissait le droit au respect de la vie privée, le droit d'exercer des recours effectifs et le droit à un procès équitable, garantis respectivement par les articles 8, 13 et 6§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Les journalistes invoquaient en outre une atteinte au secret de leurs sources et les avocats une atteinte au secret des échanges avec leurs clients.

39. Voir 8ème rapport d'activité 2023 de la CNCTR, p. 82 et suivantes.

Au terme d'une longue instruction, la Cour, dans une décision du 10 décembre 2024, rendue publique en janvier 2025[40], a jugé les différentes requêtes irrecevables, comme l'y invitait le gouvernement français, faute pour leurs auteurs d'avoir épuisé les voies de recours internes[41]. En effet, les requérants de 2015 n'avaient pas demandé à la CNCTR de s'assurer qu'ils n'avaient pas fait l'objet d'une surveillance illégale[42]. Quant aux requérants de 2017, ils avaient bien saisi la commission, puis le Conseil d'État statuant au contentieux, mais ils n'avaient pas invoqué, à l'appui de leurs recours, une violation des droits garantis par la convention.

Le mécanisme de sauvegarde que la convention a institué en créant la Cour présente un caractère subsidiaire par rapport aux systèmes nationaux de garantie des droits de l'homme[43]. Il en découle l'obligation, avant de saisir la cour, de mettre en œuvre les voies de droit ouvertes par le droit national. La décision de la cour souligne que ce principe s'impose tout particulièrement lorsqu'est en cause le secret de la défense nationale car les juridictions internes, qui ont accès aux documents couverts par ce secret, sont mieux à même de ménager l'équilibre entre les intérêts en présence.

Cependant, **cette obligation d'épuiser les voies internes ne vaut que si les recours prévus par le droit national présentent un caractère effectif**. Avant de faire droit à l'exception d'irrecevabilité opposée par le gouvernement, la cour a donc dû examiner de façon approfondie les recours ouverts devant la CNCTR puis devant le Conseil d'État[44]. Procédant à cet examen au regard des

40. Voir CEDH, 10 décembre 2024, *Association confraternelle de la Presse Judiciaire et autres*, n° 49526/15 et 13 autres requêtes, publiée le 16 janvier 2025.

41. Cette cause d'irrecevabilité est prévue par le §1 de l'article 35 de la convention qui stipule que : « *La Cour ne peut être saisie qu'après l'épuisement des voies de recours internes, tel qu'il est entendu selon les principes de droit international généralement reconnus, et dans un délai de six mois à partir de la date de la décision interne définitive.* ».

42. La possibilité de saisir la commission d'une réclamation à cette fin est prévue par les articles L. 833-4 et L. 854-9 du code de la sécurité intérieure. Voir également sur ce point la partie 2 du présent rapport p. 91 et suivantes.

43. Cette subsidiarité est consacrée par le préambule de la convention.

44. Voir les articles L 833-4 et L. 841-1 du CSI.

critères définis par de précédents arrêts[45] et s'appuyant en particulier sur les rapports d'activité de la commission, elle est parvenue à la conclusion que **le volet procédural du dispositif législatif français satisfait en tout point aux exigences de la convention.**

La cour constate d'abord que toute personne peut demander à la CNCTR de s'assurer qu'elle n'est pas surveillée illégalement au moyen d'une technique de renseignement. Elle se fonde également sur le caractère indépendant de la commission par rapport à l'exécutif, en s'appuyant sur les dispositions du code de la sécurité intérieure relatives à sa composition, à la nomination de ses membres et de son président et au caractère non renouvelable de leur mandat[46] . Il est par ailleurs rappelé que les membres et les agents qui les assistent sont habilités au secret de la défense nationale[47], disposent d'un accès permanent, complet et direct aux données issues de la surveillance et peuvent solliciter du Premier ministre tout autre élément nécessaire à l'accomplissement de leur mission[48]. Par ailleurs, si la commission ne peut pas ordonner elle-même l'interruption d'une mesure de surveillance et la destruction des éléments collectés, mais seulement formuler des recommandations en ce sens, son président ou trois au moins de ses membres peuvent former un recours contentieux devant le Conseil d'État si une telle recommandation n'est pas suivie d'effet.

La cour se penche ensuite sur le recours contentieux que les personnes qui ne se satisfont pas de la réponse de la CNCTR peuvent exercer devant le Conseil d'État[49]. Ce recours est porté devant une formation spécialisée de cette juridiction dont les

45. Voir en particulier les arrêts de Grande chambre, CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n° 58170/13, et *Centrum för rättvisa c. Suède*, n° 35052/08.

46. Voir les articles L. 831-1 et suivants du CSI.

47. Voir l'article L. 832-5 du CSI.

48. Voir notamment l'article L. 833-2 du CSI.

49. Ce recours contentieux, prévu par l'article L. 841-1 du CSI, s'exerce dans les conditions fixées aux articles L. 773-1 et suivants et R. 773-7 et suivants du code de justice administrative.

membres, ainsi que le rapporteur public, sont habilités à connaître des éléments couverts par le secret de la défense nationale. Le membre de la formation chargé d'instruire l'affaire procède aux vérifications nécessaires, sans communiquer les éléments obtenus au requérant ni à son avocat. Le jour de l'audience, si la formation de jugement entend le cas échéant leurs observations orales, elle les invite à se retirer avant que le rapporteur public ne prononce ses conclusions.

Les requérants critiquaient l'atteinte ainsi portée au principe du caractère contradictoire de la procédure, qui interdit au juge de fonder sa décision sur des éléments dont les parties n'ont pas pu prendre connaissance, ainsi qu'à l'égalité des armes. Si la cour constate en effet que la procédure déroge au droit commun en aménageant le contradictoire pour concilier les exigences du procès équitable et la préservation du secret de la défense nationale, **elle estime que cette restriction est compensée par des garanties procédurales solides**. Habilités au secret, les juges peuvent prendre connaissance de tous les éléments nécessaires pour exercer leur office, auxquels ils accèdent grâce à des pouvoirs d'instruction étendus. Par ailleurs, la CNCTR est informée du dépôt de la requête, peut présenter des observations et reçoit alors communication de l'ensemble des pièces produites par les parties. Enfin, la formation spécialisée n'est pas limitée par les moyens invoqués par le requérant mais peut soulever d'office tout moyen, contrairement à la règle normale pour la justice administrative.

Grâce à ce dispositif procédural, le Conseil d'État statue en toute connaissance de cause et peut se saisir d'illégalités que le requérant n'a pas nécessairement dénoncées, faute d'en avoir été informé. Dans le cas où elle constate une irrégularité, la formation spécialisée est en mesure d'apporter un redressement approprié en annulant au besoin l'autorisation de mettre en œuvre une technique de renseignement et en ordonnant la destruction des

éléments collectés. Si le requérant le lui demande, elle peut condamner l'État à indemniser le préjudice subi ; si elle constate une infraction, elle doit en aviser le procureur de la République.

Une autre critique des requérants concernait la motivation des décisions rendues au terme de la procédure. En effet, à l'instar des réponses adressées par la CNCTR aux réclamants qui la saisissent, ces décisions informent le requérant soit qu'aucune illégalité n'a été constatée, ce qui n'exclut pas qu'il ait fait l'objet d'une ou plusieurs techniques de renseignement dans le respect de la loi mais ce qui peut également signifier qu'il n'a fait l'objet d'aucune technique, soit qu'une illégalité a été constatée mais qu'il y a été remédié, sans précision sur la nature de cette illégalité car cette information serait de nature à porter atteinte au secret de la défense nationale.

La Cour admet que cette motivation minimale trouve une justification dans les exigences de la protection du secret de la défense nationale en rappelant que la convention européenne n'impose pas des modalités de recours qui permettraient de dévoiler aux plaignants la mise en œuvre d'une surveillance et ne fait pas obstacle à une pratique de « non-confirmation et non-dénégation ».

Ayant ainsi reconnu le caractère effectif des recours prévus par la législation française, la cour s'est interrogée sur l'existence de circonstances particulières pouvant conduire à écarter l'obligation d'épuiser les voies internes en l'espèce. En effet, les requérants auraient pu se dispenser de soumettre au Conseil d'État des moyens tirés de l'incompatibilité de la législation française avec la convention européenne dans le cas où ils se seraient heurtés à une jurisprudence contraire bien établie. Mais si le Conseil constitutionnel s'était prononcé en 2015 sur la constitutionnalité de

la législation française relative au renseignement[50], le Conseil d'État n'avait pas, à la date de présentation des requêtes devant la cour, pris parti sur sa conventionalité. Il a eu l'occasion de le faire par la suite, dans des décisions que la cour a d'ailleurs analysées dans son arrêt[51].

Ainsi, si la cour a rejeté les requêtes dont elle était saisie comme irrecevables, elle n'a pu le faire qu'en se prononçant sur **le caractère effectif des recours en matière de techniques de renseignement** et sur le **caractère équitable des règles de procédure**, consacrant le rôle déterminant de l'intervention de la CNCTR puis de la formation spécialisée du Conseil d'État en la matière et prenant, de fait, partie, dans une mesure importante, sur le fond du litige.

En revanche, sa décision ne statue pas sur les autres griefs soulevés par les requérants relatifs notamment à la protection du secret des sources des journalistes, à la liberté d'expression, au contrôle des mesures de surveillance internationale ou du recueil et de l'exploitation d'informations provenant de services étrangers. Ces questions sont toutefois éclairées par la jurisprudence de la Cour résultant d'arrêts antérieurs.

Pour l'essentiel, elles sont traitées par la législation française dans des conditions qui paraissent satisfaire aux exigences de la convention européenne. Toutefois, comme la commission a déjà eu l'occasion de le souligner à plusieurs reprises, il en va autrement en ce qui concerne le traitement par les services français des

50. Voir la décision n° 2015-713 DC du 23 juillet 2015 portant sur la loi relative au renseignement.

51. Ainsi, la formation spécialisée a jugé que le recours ouvert en matière de techniques de renseignement est un recours effectif au sens de l'article 13 de la convention (CE, 6 novembre 2017, n° 408495), que les règles applicables ne portent pas une atteinte excessive au caractère contradictoire de la procédure et à l'égalité des armes garantis par l'article 6§1 (CE, 22 mars 2024, n° 476054, point 9), que les dispositions relatives à la mise en œuvre des techniques ne méconnaissent pas le droit au respect de la vie privée garantie par l'article 8 (même décision, point 8) et que les dispositions particulières concernant les avocats, qui interdisent de les surveiller à raison de l'exercice de leur profession, ne méconnaissent ni le droit au respect de la vie privée ni les droits de la défense (CE, 22 mars 2024, n° 474404). Ces décisions prennent parti sur la conventionalité de la législation française ; par ailleurs, la formation spécialisée s'assure dans chaque dossier que les mesures éventuellement mises en œuvre répondent aux exigences de l'article 8, sans avoir à motiver ses décisions sur ce point en l'absence de violation de cet article (CE, 6 novembre 2017, n° 408495, point 7, et CE, 22 mars 2024, n° 476054, point 11).

informations fournies par des services étrangers ou symétriquement, des informations transmises à ces services par les services français[52].

## 3.2. Des modifications ponctuelles du cadre législatif du renseignement dont la portée ne peut être appréciée en l'état

Dans son précédent rapport d'activité, la CNCTR avait souligné que le rendez-vous législatif devant intervenir en 2025 pour examiner le devenir de la technique des interceptions de sécurité par la voie satellitaire, introduite à titre expérimental en 2021 dans le CSI (voir encadré en p. 48 du présent rapport) constituait une occasion de faire évoluer le cadre légal vers un meilleur respect des exigences européennes et vers plus de cohérence et d'efficacité[53]. Au vu de la décision rendue par la Cour européenne des droits de l'homme analysée ci-dessus, qui ne constate aucune méconnaissance de la convention – sans toutefois se prononcer sur tous les aspects du cadre légal français –, le gouvernement a fait le choix de ne pas présenter dans l'immédiat un projet de loi en ce sens. Dans ce contexte, ce sont donc des initiatives parlementaires, ayant chacune un objet plus circonscrit qui, respectivement, ont récemment modifié ou s'apprêtent à modifier de façon très ciblée ce cadre légal.

52. Voir notamment sur ce point le 8ème rapport d'activité 2023 de la CNCTR, p. 82 et suivantes, ainsi que le 6ème rapport d'activité 2021, p. 48 et suivantes. Voir également les actes du colloque du 15 octobre 2024, numéro 4 de la revue Etudes françaises de renseignement et de cyber (EFRC), p. 122.

53. Voir 8ème rapport d'activité 2023 de la CNCTR, p. 81 et suivantes.

### 3.2.1. La loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a étendu, à titre expérimental, la technique dite de l'algorithme[54] à de nouvelles finalités

Directement inspirée des travaux de la délégation parlementaire au renseignement sur le sujet[55] et issue d'une proposition de loi[56], la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a, par son article 6, temporairement étendu les dispositions de l'article L. 851-3 du CSI relatives à la technique dite de l'algorithme[57], aux finalités mentionnées aux 1° et 2° de l'article L. 811-3 du même code. Les traitements automatisés prévus par ces dispositions, dont l'utilisation était limitée à l'objectif de prévention du terrorisme, peuvent désormais être mis en œuvre pour détecter des connexions susceptibles de révéler des ingérences étrangères ou des menaces pour la défense nationale. Bien qu'intégrées au code de la sécurité intérieure, ces dispositions modificatives ne sont applicables que jusqu'au 31 juillet 2028[58] et devront donner lieu à un rapport au Parlement au plus tard deux ans avant cette date, de sorte qu'elles présentent un caractère expérimental.

Au 31 décembre 2024, cette possibilité nouvelle n'a pas été utilisée par les services spécialisés de renseignement (voir p. 42 du présent rapport). La commission n'est donc pas en mesure d'apprécier ses incidences concrètes en matière tant d'intensité que d'efficacité de la surveillance.

54. Voir le dossier consacré à cette technique en p. 135 et suivantes du présent rapport.

55. Voir rapport public relatif à l'activité de la DPR pour l'année 2022-2023 : https://www.assemblee-nationale.fr/dyn/16/rapports/dpr/l16b1454_rapport-information#

56. Proposition de loi n°2150 de M. Sacha Houilé, Mme Constance Le Grip et M. Thomas Gassiloud, déposée à l'Assemblée Nationale le 6 février 2024

57. Voir étude sur l'algorithme p. 135 du rapport.

58. Les dispositions des l'article 8 de la PPL narcotrafic, reportent cette échéance au 31 décembre 2028. Ce texte a fait l'objet de trois saisines du Conseil constitutionnel le 12 mai 2025. À la date de finalisation du présent rapport, la décision du Conseil constitutionnel n'est pas encore connue.

### 3.2.2. La proposition de loi visant à sortir la France du piège du narcotrafic cherche à renforcer l'usage du renseignement administratif dans la lutte contre la criminalité organisée

Les 28 et 29 avril 2025, faisant suite au rapport établi au nom de la commission d'enquête du Sénat sur l'impact du narcotrafic en France et les mesures à prendre pour y remédier[59], la proposition de loi « visant à sortir la France du piège du narcotrafic » a été adoptée par le Parlement[60]. Or, son titre III comporte des dispositions destinées à renforcer l'action des services de renseignement en matière de lutte contre le narcotrafic.

Ainsi, dans le prolongement de l'expérimentation introduite par la loi visant à prévenir les ingérences étrangères évoquées au point précédent, son article 8 a pour objet d'instituer une expérimentation tendant à étendre le recours à la technique dite de l'algorithme, prévue à l'article L. 851-3 du CSI, à une partie de la finalité mentionnée au 6° de l'article L. 811-3 du même code, soit la prévention de la criminalité et de la délinquance organisées. Il s'agit de pouvoir mettre en œuvre cette technique pour détecter des menaces « *relatives à la criminalité organisée et à la délinquance organisée portant sur des délits punis de dix ans d'emprisonnement en tant qu'elles concernent le trafic de stupéfiants, le trafic d'armes et de produits explosifs, la contrebande, l'importation et l'exportation de ces marchandises prohibées commises en bande organisée ainsi que le blanchiment des produits qui en sont issus* ».

Par ailleurs, son article 8 *bis* prolonge l'expérimentation relative à la technique des interceptions de sécurité par voie satellitaire du

59. Sénat, rapport n° 588 du 7 mai 2024, de MM. Jérôme Durain et Etienne Blanc, *Un nécessaire sursaut : sortir du piège du narcotrafic.*

60. En l'état de la numérotation du texte adopté le 28 et 29 avril par le Sénat et par l'Assemblée nationale. Ce texte a fait l'objet de trois saisines du Conseil constitutionnel le 12 mai 2025. A la date de finalisation du présent rapport, la décision du Conseil constitutionnel n'est pas encore connue.

31 juillet 2025 jusqu'au 31 décembre 2028 (voir encadré relatif à cette technique en p. 49 du présent rapport).

Enfin, dans la continuité d'une suggestion que la commission avait faite dans son précédent rapport[61], l'article 8 *ter A* a pour objet d'aligner la durée de l'autorisation d'introduction dans un lieu privé sur la durée d'autorisation de la technique dont elle est le support.

**Indépendamment des incidences que sont susceptibles d'avoir ces modifications ciblées du cadre légal, la commission observe qu'une réflexion plus transversale sur l'évolution du cadre légal, suggérée dans son précédent rapport, n'a pas encore été initiée.**

## 3.3. Concrétiser l'amélioration du contrôle *a posteriori* des recueils de données informatiques

Au-delà de certaines évolutions législatives regardées selon les cas comme indispensables ou opportunes[62] dans son rapport d'activité 2023[63], la commission avait particulièrement insisté sur **la nécessité d'améliorer le contrôle *a posteriori* des recueils de données informatiques (RDI)** tant en considération du caractère intrusif de la technique que pour prendre en compte les pratiques très diverses des services en termes de modalités de recueil et d'exploitation.

Or, force est de constater que si l'année 2024 a effectivement vu un nouvel accroissement de l'emploi de cette technique[64], les réalisations n'ont pas atteint tous les objectifs que la commission s'était fixés. Elle entend donc poursuivre résolument cet axe d'effort en 2025.

61. Voir le 8ème rapport d'activité 2023 de la CNCTR, p. 89.
62. Voir le 8ème rapport d'activité 2023 de la CNCTR, p. 81 et suivantes.
63. Voir le 8ème rapport d'activité 2023 de la CNCTR, p. 78 et suivantes.
64. Voir partie 1 du présent rapport sur l'évolution du recours à cette technique ( p. 41).

S'agissant des relations avec les services, des avancées notables avaient été obtenues en 2023. Pour un service du « premier cercle » en particulier, la commission avait obtenu que des fiches de traçabilité plus précises soient établies pour les RDI. Cette amélioration constitue un élément clé dans l'exercice du contrôle *a posteriori*, en ce qu'elle fixe clairement le cadre de recueil et permet d'identifier les éléments nécessaires à la préparation de ces contrôles, voire de détecter en amont, ces irrégularités. La démarche est à saluer puisqu'elle a permis, par exemple, d'identifier des modalités de recueil pour lesquelles les accès de la CNCTR étaient encore balbutiants, et donc de s'inscrire dans une voie de normalisation.

Cependant, la commission regrette que les éléments statistiques attendus n'aient pu faire l'objet d'une transmission régulière durant l'année 2024. Leur disponibilité ponctuelle, si elle a confirmé la capacité du service concerné à encadrer la mise en œuvre de modalités spécifiques, n'a pas pleinement contribué au développement des processus de contrôle *a posteriori* de la commission, laissant une situation encore en partie inachevée.

S'agissant du développement d'outils d'exploitation centralisée, ce sujet est sans aucun doute celui qui a suscité le plus d'échanges au cours de l'année 2024 avec la communauté du renseignement.

Ainsi que le rapportait la commission l'année dernière, le Président de la République a demandé la mise en place d'une solution facilitant le contrôle *a posteriori* des RDI par la commission. Reporté à l'issue des Jeux olympiques et paralympiques, le lancement du projet a bien eu lieu en octobre 2024, sous l'égide de la Coordination nationale du renseignement et de la lutte contre le terrorisme.

Au regard de l'état d'avancement de ce projet et des exigences tenant à la protection du secret de la défense nationale, la commission est en mesure de rendre compte des éléments suivants.

Tout d'abord, elle se félicite d'être largement associée à la conception et à la conduite du projet et appelle naturellement à sa poursuite ; elle gage que cette situation résulte notamment du renforcement de ses compétences techniques, impulsées par le président Lasvignes. Elle est désormais reconnue comme une interlocutrice légitime dans les échanges, quelle que soit leur technicité. Les travaux réalisés depuis le mois d'octobre 2024 ont permis de clarifier le périmètre du projet, au-delà des orientations données et des déclarations d'intention initiales. Si celui-ci est donc aujourd'hui tout à fait initié, la commission sera vigilante sur le respect du calendrier prévu, qui comporte une réalisation effective en 2027.

Sur l'objectif et le fond du projet, si les modalités d'exécution du contrôle à distance de la CNCTR ont évolué depuis les premières ébauches menées fin 2023, son effectivité est une condition *sine qua non* et les propositions d'architecture formulées à ce stade satisfont ce critère.

**Des points de complexité ont été clairement identifiés et la commission sera vigilante pour que le projet se poursuive dans des conditions satisfaisantes**. Elle est en effet résolument engagée dans l'aboutissement de cette démarche aux côtés des autres partenaires du projet. Il s'agit d'un levier majeur pour renforcer son contrôle *a posteriori* des RDI. L'année 2025 devra donc absolument conforter cette trajectoire initiale, afin de disposer en 2027 d'un système opérationnel.

Enfin, **la commission rappelle l'intérêt qu'elle voit à la mise en œuvre, par un service important, des dispositions qu'il s'était engagé à prendre pour faciliter l'accès aux bulletins de renseignement tirés de l'exploitation de RDI dans l'attente d'un système plus global**.

## LES 10 ANS DE LA CNCTR

***« La CNCTR est au cœur de la démocratie. […] La CNCTR est une instance essentielle à la vitalité de notre démocratie, à la préservation de nos libertés, à la conciliation entre la sécurité, l'efficacité des services et la préservation des droits et libertés individuels ».***

*M. Loic Kervran*, député du Cher[65]

***« La CNCTR joue donc un rôle considérable dans la régulation des services de renseignement ».***

*M. Guillaume Larrivé*, ancien député de l'Yonne[66]

**Le 3 octobre 2025[67] marquera les 10 ans d'existence effective de la Commission nationale de contrôle des techniques de renseignement.**

Au cours de cette décennie, la CNCTR a su s'imposer comme un acteur essentiel dans le paysage du renseignement français, assurant un contrôle rigoureux et aussi transparent que possible, dans le respect des exigences de protection du secret de la défense nationale, des activités des services de renseignement encadrées par le code de la sécurité intérieure. Conformément aux principes fixés par la loi, ce contrôle a pour objectif d'assurer un équilibre entre protection des libertés individuelles et préservation des intérêts fondamentaux de la Nation.

**À l'occasion de cet anniversaire, la commission organisera un colloque le 22 septembre 2025.**

65. Audition de M. Serge Lasvignes devant l'Assemblée nationale, le 22 septembre 2021.

66. *idem.*

67. Date d'effet des nominations des différents membres du premier collège de la commission.

# Les outils de la surveillance

# Dossier 1. Les matériels permettant de porter atteinte à la vie privée

## Étude : Le charme discret des articles R. 226-1 et suivants du code pénal : L'encadrement de la commercialisation et de la détention des matériels pouvant permettre de commettre des atteintes à la vie privée et ses enjeux

Le législateur français a fait le choix en 2015, dans le cadre de la loi du 24 juillet 2015 relative au renseignement[1], de concevoir et organiser le contrôle de l'activité des services de renseignement à travers le prisme de techniques de renseignement limitativement prévues par le code de la sécurité intérieure.

Cependant, l'existence d'une autorisation légale de mise en œuvre d'une technique, que ce soit une interception d'une communication téléphonique, ou un recueil des données stockées dans un système informatique, serait dépourvue d'effets si elle ne se doublait pas de la possibilité, pour le service, de réaliser techniquement ces opérations. Autrement dit, sans les moyens de

1. Loi n° 2015-912 du 24 juillet 2015.

surveiller, l'autorisation de surveiller est dépourvue de sens. Or la possibilité concrète des services de renseignement à mettre en œuvre les techniques autorisées dépend de plus en plus du maintien d'un niveau capacitaire proportionné au développement actuel des technologies en matière de communications électroniques, voire de façon plus générale, en matière d'outils numériques.

La portée réelle d'une autorisation de mise en œuvre d'une technique de renseignement ne peut donc être pleinement appréciée sans considérer également les fonctions et le statut des outils de surveillance et d'interception qu'elle mobilise. Il en va ici, au-delà des questions étroitement juridiques, de la structure et de la dynamique d'un marché particulier, celui des technologies de surveillance.

La commission consultative instituée par l'article R. 226-2 du code pénal[2], dont le secrétariat est assuré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en délivrant les autorisations notamment nécessaires à la fabrication, à la vente ou à l'acquisition de matériels permettant d'effectuer les surveillances techniques prévues au livre VIII du code de la sécurité intérieure, se situe ainsi au carrefour de deux dimensions essentielles.

D'une part, son existence traduit la volonté de fournir à la protection de la vie privée un ensemble continu et cohérent de garanties juridiques. Face à un marché technologique où les zones grises se multiplient, l'acquisition « sur internet » de capacités techniques relevant du régime contrôlé est parfois déconcertante de simplicité, y compris sur des sites marchands grand public, la commission dite « R. 226 » constitue l'unique instance structurant ce secteur en France.

2. L'ensemble des dispositions du code pénal mentionnées dans l'étude figurent en annexe 5 du présent rapport.

D'autre part, en délivrant des autorisations différenciées selon que l'utilisateur final de tels dispositifs est habilité à produire du renseignement au sens du code de la sécurité intérieure, ou justifie d'autres titres à un tel usage, la commission « R. 226 » contribue au contrôle de la puissance publique comme à la régulation du marché privé. À ce double titre, c'est bien le soubassement matériel de la surveillance qui est soumis à l'examen, et interrogé conformément aux fins que se propose un État de droit.

La présente étude entend ainsi montrer simultanément la nécessité et la pertinence du cadre légal en vigueur, comme la manière dont la Commission nationale de contrôle des techniques de renseignement (CNCTR) contribue, avec l'ensemble des partenaires impliqués, à la maîtrise de technologies en constante évolution.

# 1. Le contrôle exercé par la commission « R. 226 » s'inscrit dans la continuité des missions dévolues à la CNCTR en matière de protection de la vie privée et d'encadrement des techniques de surveillance

## 1.1. L'instauration d'un dispositif d'autorisation réglementaire rigoureux en matière de technologies de surveillance est une condition de la protection de la vie privée

### 1.1.1. Les différents usages de dispositifs techniques rendant possible l'interception des correspondances, des données ou des paroles tenues à titre privé constituent des délits en l'absence d'une base légale évaluée par la commission consultative « R. 226 »

Le code pénal définit plusieurs infractions relatives à l'atteinte à la vie privée. Il est notamment interdit de capter, enregistrer ou transmettre, sans le consentement de la personne concernée, des paroles prononcées à titre privé ou confidentiel, ou de fixer, enregistrer ou transmettre l'image d'une personne se trouvant dans un lieu privé. L'introduction dans un domicile privé, le recueil de données informatiques personnelles ou la géolocalisation d'une personne à son insu, de même que la conservation et le partage d'informations rassemblées par ces différents moyens, constituent

également des délits. Par extension, d'une part la fabrication, l'importation, l'exposition, l'offre, la location et la vente, d'autre part l'acquisition et la détention, d'appareils de nature à permettre ou faciliter la commission de ces différentes atteintes à la vie privée, qu'il s'agisse de micros directionnels, de caméras miniaturisées ou encore de dispositifs d'interception des communications téléphoniques, tombent également sous le coup de la loi.

L'article 226-3 du code pénal sanctionne spécifiquement trois « intrusions techniques » dans la vie privée :

- l'accès aux communications électroniques (voir l'article 226-15 du code pénal),
- la captation de paroles prononcées à titre privé (voir l'article 226-1 du code pénal),
- et la captation de données informatiques (par référence aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure).

Cet article dispose en outre que l'infraction peut être visée y compris lorsque les faits constitutifs sont commis par négligence, « en l'absence d'autorisation ministérielle ».

Il encadre enfin la publicité pouvant être réalisée, laquelle ne doit pas constituer une incitation à commettre les infractions précitées.

Les surveillances administratives comme judiciaires impliquent nécessairement des atteintes à la vie privée et sont donc, par principe, dérogatoires au droit commun, qui entoure l'intimité et l'existence privée de chacun de multiples garanties.

Il y a lieu à cet égard de relever que le livre VIII du code de la sécurité intérieure s'ouvre sur l'exception régalienne qui permet de justifier qu'il soit porté atteinte au respect de la vie privée « *dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de*

*proportionnalité* » (voir l'article L. 801-1 du CSI) et fonde l'existence d'une « *politique publique de renseignement* » menée par les services pour la poursuite de finalités limitativement énumérées au titre desquelles une telle atteinte est légitime (voir les articles L. 811-1 à L. 811-3 du même code).

Le même souci de cohérence, qui conduit le code pénal à lier la sanction des atteintes à l'intimité et le commerce des moyens permettant leur mise en œuvre, implique également que les services de renseignement justifient d'une autorisation légale à la détention des appareils leur permettant de réaliser les missions qui leur sont fixées.

Un régime d'autorisation est ainsi mis en place au sein du code pénal afin de contrôler, d'une part, la mise sur le marché de ces dispositifs (article R. 226-3 du code pénal), d'autre part, leur acquisition par des entités privées ou publiques (article R. 226-7 du code pénal). Cette interprétation globale des dangers, comme de la nécessité de la surveillance, de ses intentions, aussi bien que ses moyens, constitue à cet égard une singularité française que la commission consultative « R. 226 » a la charge de faire vivre.

### 1.1.2. La commission consultative « R. 226 » assure un suivi de ces dispositifs tout au long de leur cycle de vie et d'utilisation

**L'article R. 226-2 du code pénal institue la commission consultative chargée d'éclairer le directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)**, auquel revient *in fine* la responsabilité de délivrer les autorisations de commerce et

d'acquisition de dispositifs dont la nature est précisée par arrêté[3]. Sa composition, fixée par le même article à onze membres, traduit sa forte dimension interministérielle, avec des représentants des ministères de la justice, de l'intérieur, des armées et de l'économie, et son ouverture aux autorités administratives (la CNCTR et l'Agence nationale des fréquences, ANFr, sont ainsi représentées) et à l'expertise technique (deux personnalités qualifiées sont nommées par le Premier ministre).

Cette commission évalue chaque dispositif de surveillance, matériel ou logiciel, dans tous les aspects de son cycle de vie, et selon la nature de la demande soumise. Qu'il s'agisse d'importer un dispositif de captation de données sur le territoire national, d'en faire la démonstration lors d'un salon spécialisé, ou d'en faire usage au sein d'un service de renseignement, une autorisation doit être délivrée par le directeur général de l'ANSSI, sur avis de la commission consultative « R. 226 ». La procédure prévue par l'article R. 226-4 du code pénal implique que l'appareil concerné fasse l'objet d'une présentation technique, voire d'une expertise complète, afin d'en cerner les usages, les risques, ainsi que le marché auquel il a vocation à s'adresser. L'autorisation délivrée est ensuite modulée dans sa durée, pouvant aller jusqu'à six ans, comme dans son périmètre, avec le cas échéant des restrictions d'usages, et l'instauration d'une traçabilité de l'appareil d'après son numéro d'autorisation (article R. 226-6).

La haute technicité des dispositifs soumis à l'appréciation collégiale, de même que les enjeux importants s'agissant de la protection de la vie privée, supposent un suivi rigoureux des demandes, dont le secrétariat est assuré par l'ANSSI. La possibilité pour la commission de réserver son avis, de le subordonner à des présentations par les entreprises la sollicitant, permet en outre de délivrer des autorisations sur la base de l'information la plus

3. Cette liste indique les différentes catégories de matériels soumises aux autorisations « R. 226 ». La commission doit en premier lieu apprécier, dans chaque cas, si un dispositif précis, soumis par un industriel sollicitant, par exemple, une autorisation de vente sur le territoire national, relève effectivement de cette liste. Le dernier arrêté en vigueur est l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévues par l'article 226-3 du code pénal.

complète possible. À raison, en moyenne, d'une réunion tous les deux mois, ce sont ainsi environ 1500 autorisations délivrées chaque année, au sens des articles R. 226-3 et R. 226-7 du code pénal[4]. Ces avis dessinent progressivement une doctrine au cœur de la régulation publique des technologies de surveillance et d'interception.

## 1.2. Les dispositions des articles R. 226-1 et suivants du code pénal offrent à la CNCTR une modalité supplémentaire de contrôle de l'activité des services de renseignement

### 1.2.1. Si les services de renseignement ont par définition vocation à employer les dispositifs visés par les articles R. 226-1 et suivants du code pénal, et bénéficient d'un régime d'autorisation spécifique, leurs usages et leurs inventaires font l'objet de contrôles par la CNCTR

La commission « R. 226 », on l'aura compris, a une mission plus large que l'encadrement des services de renseignement. Elle constitue en effet d'abord un point de passage obligé pour quiconque entend pénétrer à un titre quelconque sur le marché de la surveillance en France. Il va de soi toutefois que les services de renseignement, sans pour autant qu'ils puissent déroger à l'obligation de disposer des autorisations idoines pour l'équipement dont ils usent, prennent une place particulière dans cette économie.

4. Voir interview de M. Vincent Strubel, p. 129 et suivantes du présent rapport. Les rapports d'activité de l'ANSSI font état de 1567 décisions rendues en 2023 dont 22 décisions refus et de 1610 décisions rendues en 2024 dont 52 décisions de refus.

Les services de l'État peuvent en effet bénéficier d'une facilité de formalisme. Tenant compte, le cas échéant, de leur légitimité à utiliser de tels appareils en application de la loi, la sollicitation de demandes unitaires pour chaque dispositif détenu est remplacée par la tenue dans chaque service d'un registre, accessible à la CNCTR, traçant l'intégralité des équipements en possession de l'entité. Cette autorisation, dite « de plein droit » (APD, prévue à l'article R. 226-9 du code pénal), est réévaluée à échéance régulière[5] en séance formelle, dont la composition est limitée à l'ANSSI et à la CNCTR pour des questions de sensibilité des informations échangées. Sont en particulier examinées à cette occasion l'organisation du service pour la gestion et le suivi des équipements, la qualité du registre, toute évolution de la base légale s'agissant de l'emploi de ces capacités et l'absence d'anomalie sur la période écoulée.

De façon connexe, le code de la défense prévoit et encadre la mise en œuvre sur le territoire national d'appareils, aux seules fins d'essais, par certaines unités relevant du ministère des armées. La CNCTR est là aussi placée en position de contrôle de ces opérations ; l'article L. 2371-2 du code de la défense dispose ainsi que de telles activités sont soumises à une déclaration préalable à son attention[6]. Cette dernière est ainsi en capacité de vérifier à la fois les conditions d'acquisition et de détention des matériels de collecte du renseignement, et les modalités de leur mise en œuvre, au cas par cas, que ce soit dans le cadre des autorisations délivrées par le Premier ministre au titre du livre VIII du code de la sécurité intérieure ou pour des essais.

5. En pratique tous les trois ans, soit à la même échéance que pour toute demande d'acquisition/détention.

6. Article L. 2371-2 du code de la défense : « *Sous réserve d'une déclaration préalable à la Commission nationale de contrôle des techniques de renseignement, le service du ministère de la défense chargé de la qualification des appareils ou des dispositifs techniques mentionnés au 1° de l'article 226-3 du code pénal au profit des armées et des services du ministère de la défense, d'une part, et les militaires des unités des forces armées définies par arrêté du ministre de la défense, d'autre part, sont autorisés à effectuer des essais des appareils ou dispositifs permettant de mettre en œuvre les techniques ou mesures mentionnées à l'article L. 851-6, au II de l'article L. 852-1 ainsi qu'aux articles L. 852-2, L. 854-1 et L. 855-1 A du code de la sécurité intérieure. Ces essais sont réalisés par des agents individuellement désignés et habilités, à la seule fin d'effectuer ces opérations techniques et à l'exclusion de toute exploitation des données recueillies. Ces données ne peuvent être conservées que pour la durée de ces essais et sont détruites au plus tard une fois les essais terminés. / La Commission nationale de contrôle des techniques de renseignement est informée du champ et de la nature des essais effectués sur le fondement du présent article. À ce titre, un registre recensant les opérations techniques réalisées est communiqué, à sa demande, à la commission. / Les conditions d'application du présent article sont fixées par arrêté du ministre de la défense, pris après avis de la Commission nationale de contrôle des techniques de renseignement.* »

### 1.2.2. Les activités de la commission consultative « R. 226 » sont pour la CNCTR une occasion d'aborder sous un angle spécifique, simultanément technique, économique et juridique, les grands enjeux du cadre légal

La CNCTR veille à ce que les techniques de renseignement limitativement prévues par le code de la sécurité intérieure soient mises en œuvre dans le respect de leur cadre légal. La dimension transversale de la surveillance, notamment dans l'environnement numérique contemporain, impose néanmoins que le contrôle indépendant qu'elle exerce se nourrisse d'approches multiples, irréductibles au seul formalisme juridique.

La CNCTR contribue aux délibérations de la commission consultative « R. 226 » en y apportant son expertise juridique, s'agissant des atteintes à la vie privée ou des enjeux de police administrative propres à l'activité des services de renseignement. En retour, elle profite des présentations et des débats pour actualiser sa propre compréhension des enjeux technologiques sous-jacents à l'emploi des techniques listées par le chapitre V du livre VIII du code de la sécurité intérieure. La diversité, tant des matériels examinés que des scénarios d'emploi associés[7], offre à la commission la possibilité d'élargir sa connaissance des outils de la surveillance et par ce biais d'assurer une veille technologique efficace sur les nouvelles modalités techniques, qui complète utilement les échanges qu'elle développe avec les services de renseignement.

7. Un même produit peut être utilisé pour des finalités et dans le cadre de périmètres réglementaires tout à fait distincts.

La commission « R. 226 », au-delà de son appellation administrative, constitue dès lors un espace original où poursuivre le dialogue avec les services de renseignement à partir d'objets différents, au plus près de leurs préoccupations opérationnelles mais aussi budgétaires. Elle permet également de mettre à jour des difficultés propres aux évolutions de l'économie de l'information, lorsque celle-ci rencontre des enjeux de souveraineté, à l'instar de l'essor du marché intérieur européen des opérateurs de télécommunications.

# 2. Le développement et la diffusion des moyens technologiques relevant de la réglementation dite « R. 226 » n'a pas pris de vitesse un cadre légal qui demeure adapté et opératoire pour les autorités de contrôle

## 2.1. Le régime strict d'autorisation prévu par le code pénal conduit à un dialogue étroit de la commission « R. 226 » avec les acteurs de la production, de la commercialisation et de la mise en œuvre des appareils et dispositifs concernés

### 2.1.1. La délivrance d'autorisation s'effectue au terme d'un dialogue parfois étendu avec les industriels, les distributeurs et les utilisateurs des dispositifs concernés

La commission consultative « R. 226 » se réunit principalement aux fins d'examiner les demandes d'autorisation qui lui sont soumises. Elle rend ainsi plusieurs centaines d'avis lors des six réunions généralement programmées chaque année. Dans le cadre de ces réunions, elle suit également, de façon collégiale, l'avancement de dossiers à plus long cours pouvant affecter l'appréciation qu'elle porte sur certaines catégories d'équipements. La commission se saisit des problématiques d'atteinte potentielle à la vie privée que représentent les produits disponibles sur le marché et est amenée, le cas échéant, à prendre des décisions de classement. Dès lors,

chacune des étapes (fabrication, importation, exposition, offre, location, vente, acquisition, détention) est soumise à l'obtention d'une autorisation.

À titre d'exemple, la commission consultative a proposé en 2022 le classement des matériels d'investigation numérique sur les téléphones mobiles, qui sont notamment utilisés par les services d'enquête ou les experts judiciaires, au regard de l'usage que tout un chacun fait aujourd'hui de son téléphone portable et des fonctionnalités sans cesse renforcées de ces appareils.

Outre cette activité régulière, la commission s'entretient directement avec certains demandeurs afin qu'ils précisent leurs sollicitations. S'agissant d'industriels ou de fournisseurs, il est parfois nécessaire d'obtenir des informations techniques détaillées, par exemple sur la liste des données recueillies ou encore sur les performances escomptées selon les scénarios d'emploi. Dans le cas des demandes d'acquisition, la commission est vigilante à la base légale invoquée pour justifier de la détention des appareils. Ainsi, il est courant de solliciter des précisions complémentaires auprès des entités, qu'elles soient privées ou publiques, afin qu'elles décrivent le cadre d'emploi, les textes applicables, mais aussi les conditions de stockage et le suivi logistique des matériels pour prévenir tout mésusage.

### 2.1.2. La commission « R. 226 » s'appuie dans ses avis sur des profils d'usages évaluant dans chaque cas l'ampleur du caractère intrusif du dispositif analysé

Dans sa démarche d'analyse des équipements, la commission « R. 226 » s'attache tout d'abord à apprécier si ceux-ci permettent de commettre les infractions prévues par le code pénal précédemment mentionnées et, le cas échéant, si leur objet même est de permettre la commission de ces infractions. Selon les résultats de cette évaluation, le matériel sera ainsi classé, ou non,

comme relevant de la réglementation « R. 226 » et soumis à autorisation, quel que soit son utilisateur potentiel et la légitimité de son activité. Pour autant, en fonction de l'ampleur du caractère intrusif du matériel considéré, certains sont rendus accessibles uniquement à certains utilisateurs au regard des missions qui leur sont confiées par la loi.

Ensuite, un demandeur, représentant éventuellement une personne morale, peut solliciter du directeur général de l'ANSSI une des autorisations listées précédemment. La commission évalue alors le fondement légal de la demande mais également les risques qui seraient induits par la délivrance de l'autorisation. *In fine*, l'ANSSI délivre, ajourne ou refuse l'autorisation, se fondant sur les avis de la commission consultative, construits notamment sur les principes de nécessité et de proportionnalité.

L'évaluation de la nécessité repose en premier lieu sur l'analyse des bases légales que le demandeur peut faire valoir. Ainsi, pour un service de l'État, il est régulier qu'une disposition législative ou réglementaire permette de justifier le recours à des dispositifs techniques visés par le régime d'autorisation « R. 226 ». Le type de dispositif peut parfois être explicitement cité ou découler logiquement de l'adéquation entre un processus encadré et une cible technique. Dans le cas contraire, la commission s'attache à apprécier la recevabilité de la demande en tenant compte des pratiques du secteur d'activité concerné et des enjeux ; la démarche s'appuie souvent sur des consultations plus larges.

La commission, recherchant une action à la fois cohérente et robuste, a défini des profils d'usage. Ils ont pour objectif d'assurer la protection des libertés individuelles sans entraver abusivement les acteurs économiques concernés. Ces profils s'appuient sur la diversité des équipements mis sur le marché. Ainsi pour une même finalité technique, plusieurs catégories de produits se distinguent parfois. Prenant l'exemple de l'investigation numérique, un dispositif

qui réaliserait la seule copie des données n'aurait pas la même potentialité intrusive qu'un dispositif qui permettrait à la fois le contournement de protections de la vie privée (tels qu'un code de déverrouillage ou un mot de passe) et la copie des données. En effet, dans le premier cas, l'accès à la donnée serait subordonné à la communication préalable d'un secret personnel, pouvant signifier l'information et l'accord préalables du propriétaire. Partant, la commission évalue la proportionnalité entre l'usage justifié et l'ampleur du caractère intrusif de l'équipement sollicité.

Il y a à cet égard une certaine continuité entre les questions de proportionnalité soumises au quotidien à la CNCTR dans le traitement des demandes de techniques de renseignement par les services, d'une part, et l'appréciation du degré d'atteinte à la vie privée dont est porteur un dispositif particulier devant la commission « R. 226 », d'autre part.

## 2.2. Le contrôle administratif et judiciaire des appareils relevant des articles R. 226-1 et suivants du code pénal, loin d'entraver l'innovation, contribue à la structuration et à l'efficience de ce marché

### 2.2.1. Les infrastructures et dispositifs nécessaires à la surveillance technique ne cessent de se développer et de se complexifier, sans pour autant frapper d'obsolescence le cadre légal

À l'instar des algorithmes, il est tentant de regarder le développement du marché de la surveillance comme l'expression d'une menace obscure, hautement technique et très dynamique

face à laquelle la loi serait sans force. Le dynamisme du secteur industriel est incontestable. Il se déploie dans plusieurs directions et à de multiples échelles : mécanismes d'interceptions destinés aux opérateurs de télécommunication afin de satisfaire aux réquisitions prévues par la loi[8] ; dispositifs matériels ou logiciels, « *spécifiquement conçus pour, sans le consentement des intéressés, accéder aux données informatiques, les enregistrer, les conserver et les transmettre* »[9] ou encore « *appareils d'interception du son à distance de type microcanon ou équipés de dispositifs d'amplification acoustique* »[10]. Le spectre des dispositifs relevant de la réglementation « R. 226 » est ainsi large et en constante évolution.

Toutefois et indépendamment même de la prolifération technologique, la procédure présentée précédemment constitue une étape structurante pour les acteurs, privés comme publics, intervenant sur ce marché, en assurant leur sécurité juridique respective. En ce sens, les craintes légitimes qui peuvent naître de la relative « démocratisation » de l'accès à ces appareils doivent être tempérées.

D'une part, la caractérisation technique des dispositifs pertinents s'élabore au niveau de l'arrêté précité et peut donc être aisément mise à jour par le Premier ministre, sans nécessiter la refonte du code pénal à chaque innovation technologique. D'autre part, le traitement en un point unique des autorisations nécessaires à la diffusion licite de ces appareils rend possible une approche transversale du marché. L'absence de délai légal à la délivrance ou au refus d'une autorisation permet à cet égard à la commission de prendre le temps nécessaire à l'évaluation des nouveaux dispositifs.

8. Voir arrêté du 11 août 2016, modifiant l'arrêté du 4 juillet 2012 cité note 3 ci-dessus.
9. Voir point 3 de l'annexe I à l'arrêté du 4 juillet 2012 cité note 3 ci-dessus.
10. Voir point 2 de l'annexe I à l'arrêté du 4 juillet 2012 cité note 3 ci-dessus.

### 2.2.2. Le régime d'autorisation permet à ce marché et à ces technologies de maîtriser le risque judiciaire clairement énoncé par le code pénal, tout en constituant un levier important dans la protection de la vie privée et des libertés individuelles

La régulation publique des technologies de surveillance, telle qu'y contribue la commission consultative « R. 226 », se concentre principalement dans la phase d'autorisation initiale. C'est en effet au moment de la soumission d'une demande de mise sur le marché, de fabrication ou de cession, le cas échéant, que les pouvoirs publics ont l'opportunité d'évaluer les dangers inhérents à un dispositif technique. Le contrôle *a posteriori* soulève pour sa part des difficultés spécifiques, notamment au regard des moyens judiciaires conséquents qu'impliquerait le contrôle systématique des autorisations rendues.

Toutefois, il faut noter, d'une part, que ce contrôle existe et peut prendre une valeur clairement dissuasive, par exemple lorsque l'exposition illicite de matériels non autorisés lors d'un salon conduit au placement immédiat des exposants en garde à vue et à la saisie des produits. Le risque légal est donc clairement exprimé et présent à l'esprit des différents acteurs de ce marché particulier. Pour une entreprise spécialisée dans la conception et la commercialisation d'appareils de surveillance, le maintien de l'autorisation légale dont le législateur a explicitement prévu le retrait (voir article R. 226-11 du code pénal), peut constituer une menace existentielle en lui interdisant l'accès au marché français.

D'autre part, on l'a dit, les dispositifs relevant de la réglementation « R. 226 » participent à l'efficacité même des services de renseignement et sont donc pleinement inscrits dans le périmètre du contrôle que la CNCTR exerce à leur égard. La possibilité de

demander des comptes, lors d'un contrôle sur place, de l'usage d'un dispositif dont la traçabilité, le numéro de série, sont directement accessibles à la CNCTR apparaît comme un outil significatif pour crédibiliser l'intensité et la précision de ce contrôle. Plus largement, les différentes autorités publiques susceptibles de solliciter l'acquisition de dispositifs similaires, en dehors de la sphère étroite des services de renseignement, savent devoir se plier à la procédure consultative d'une commission dont le pluralisme favorise l'impartialité.

Sous ces différents aspects, le cadre légal dans lequel opère la commission « R. 226 » donne des instruments pertinents pour encadrer le développement de technologies dont la prolifération sauvage pourrait présenter des menaces sérieuses à l'égard de la vie privée.

# Interview de M. Vincent Strubel, directeur général de l'ANSSI

**Pouvez-vous rappeler brièvement les missions de l'ANSSI et positionner plus spécifiquement l'activité R. 226 dans cet éventail ?**

Sous l'autorité du Premier ministre et rattachée au Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), l'ANSSI bénéficie d'un positionnement lui permettant de déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle. Cette politique s'attache à défendre les infrastructures numériques publiques et privées les plus critiques. Elle s'adresse également à l'ensemble des acteurs de la transformation numérique de la France et favorise les conditions d'un dialogue de confiance avec ses homologues à l'échelle européenne et internationale.

L'ANSSI est également en charge du régime de contrôle dit « R. 226 », découlant de l'article 226-3 du code pénal. À ce titre, et en lien avec la commission consultative (« Commission R. 226 ») instaurée par l'article R. 226-2 de ce même code, elle étudie les demandes de commercialisation et de détention des produits susceptibles de porter atteinte au secret des correspondances et à

la vie privée. Elle veille ainsi à ce que ces produits présentent un niveau de sécurité suffisant pour éviter tout détournement de leur usage, et ne soient mis à la disposition que des seuls acteurs auxquels la loi confère un usage légitime de tels produits.

**Quelles sont les ressources mobilisées par l'agence pour cette activité ?**

Le secrétariat de la Commission R. 226, piloté par le bureau des contrôles réglementaires de l'ANSSI, assure l'instruction administrative des dossiers déposés. Leur analyse sur le plan technique mobilise, en fonction des besoins, de nombreuses expertises réparties au sein de l'ANSSI, en particulier celles du bureau sécurisation des communications, spécialisé dans l'analyse et la sécurisation des réseaux de télécommunications.

**Est-il possible d'évoquer succinctement les types de produits les plus régulièrement examinés par la Commission consultative ?**

Jusqu'à une époque récente, la plupart des dossiers étudiés par la Commission R. 226 concernaient deux grandes familles :

- produits de télécommunications (routeurs, outils d'analyse de trafic, sondes, etc.), et dispositifs d'interception mis en œuvre au profit des services de l'État (parties intégrantes des réseaux de communications électroniques) ;

- dispositifs d'interception mis en œuvre par les services de l'État et les armées, moyens de contrôle du spectre radio et matériels dits « de dépoussiérage » (type scanners).

La fin des années 2010 ayant vu le développement des dispositifs d'analyse forensiques[11] accessibles au grand public et présentant pour certains la capacité de « déverrouiller » des terminaux informatiques sans le consentement de leurs utilisateurs légitimes,

11. Désigne l'investigation numérique légale. Elle a pour objectif de produire une preuve numérique (sa collecte, son analyse et sa conservation) dans le cadre d'une action en justice.

la commission a étendu en 2019 son activité au contrôle de ces dispositifs, afin d'en limiter l'usage aux seuls acteurs légitimes au regard du droit français, compte tenu de leurs capacités très intrusives.

**Quel volume de décisions portées à votre signature cela représente-t-il par an ?**

Le nombre de décisions est en augmentation régulière depuis 2019, avec environ 270 à 350 produits étudiés par séance. Sur les cinq dernières années, 7 749 décisions ont été rendues, soit une moyenne de 1 550 par an.

**Avez-vous une visibilité sur les approches réglementaires développées par nos partenaires ? Sont-elles comparables au régime de contrôle institué par le Code pénal, ou à l'inverse la France déploie-t-elle un encadrement tout à fait original ?**

Ce dispositif est spécifique à la France, et n'a pas d'équivalent naturel chez nos partenaires même les plus proches. Cependant, certains de ces partenaires ont montré leur intérêt pour notre réglementation, notamment au regard de l'impact positif qu'elle a eu sur la sécurité des réseaux de nos opérateurs de communications électroniques.

**Le cadre légal réserve à la Commission consultative R. 226 une place dans la régulation initiale des dispositifs classés, une extension du contrôle *a posteriori* vous paraît-elle souhaitable voire nécessaire ? Quelles formes celle-ci pourrait-elle prendre ?**

En tout état de cause, la logique voudrait qu'une instance effectuant un contrôle *a priori*, basé sur les dispositions d'articles du code pénal, l'effectue également *a posteriori*. L'instruction interministérielle du 5 septembre 2006 inclut le contrôle dans les compétences de la commission R. 226 (§3 de l'art. 2). À l'heure actuelle, les contrôles *a posteriori* sont effectués par les ministères de l'intérieur et des armées ainsi que par la direction nationale du

renseignement et des enquêtes douanières (cette dernière au titre du code des douanes). La CNCTR assure pour sa part les contrôles des services de renseignement.

Les agents de l'ANSSI, qui ne disposent pas de pouvoirs de police judiciaire, n'ont pas vocation à effectuer seuls de tels contrôles. Ils peuvent néanmoins épauler ces différents services, en apportant une expertise technique, y compris lors de contrôles sur place. De telles équipes mixtes ont déjà été mises en œuvre lors de contrôles menés à l'occasion de salons professionnels spécialisés.

**Le rôle de régulateur expose souvent à des tentatives de pressions ou d'orientations de la part des intérêts constitués. Quel rapport la Commission R. 226 entretient-elle avec les secteurs économiques concernés ? Comment son autorité est-elle perçue ?**

En règle générale, l'autorité de la commission est bien acceptée, tant par l'administration que par les industriels et usagers privés. Les échanges avec les industriels des télécommunications et des produits « sensibles » sont fluides, notamment grâce à l'accompagnement administratif et technique de l'ANSSI et du Commissariat aux communications électroniques de défense (CCED).

La relation est particulièrement étroite avec les opérateurs de communications électroniques, qui sont la cible de nombreuses tentatives de cyberattaques et ont bien intégré que les contrôles menés au titre du R. 226 sont une source d'amélioration continue de leur niveau de sécurité. Ils ont ainsi intégré l'instruction de leurs demandes R. 226 dans une démarche d'anticipation, facilitant le test par l'ANSSI des équipements dont ils envisagent le déploiement.

**Le cadre légal demeure opérant malgré les rapides évolutions technologiques du domaine. Anticipez-vous toutefois des transformations plus lourdes qui pourraient impacter directement le modèle national ?**

Les changements majeurs induits par la technologie 5G, comme la conteneurisation ou l'utilisation de *clouds* de télécommunications internes développés et maintenus par les opérateurs de communications électroniques (OCE), rendent de plus en plus difficile de voir une fonction réseau comme un « appareil » au sens de la réglementation R. 226 (socles et logiciels métiers sont interdépendants). Ce point à lui seul nécessiterait une évolution du cadre réglementaire.

Les autres besoins identifiés concernent le satellitaire, les réseaux radio mobile privée (PMR) ou encore les réseaux transfrontaliers/pan-européen, ainsi que la nécessité de gérer l'entrée de certains acteurs sur des fonctions particulières (RCS/iMessages). On peut aussi ajouter la réorganisation du marché avec une place grandissante des opérateurs d'infrastructures mobiles passives (*TowerCo*) qui pourraient se positionner en *RAN as a Service* (la gestion des antennes et des BTS n'est plus assurée par l'opérateur, et est potentiellement mutualisée au niveau *vRAN* plutôt qu'en *RAN sharing*). Certaines lignes de partage devraient sans doute aussi être mieux formalisées, notamment sur ce qui devrait être fait côté IT[12] et OTT[13].

Enfin, il conviendrait d'anticiper le souhait exprimé par la Commission européenne d'uniformiser le cadre réglementaire dans un objectif de marché unique, ce qui pourrait conduire à une révision des régimes nationaux d'autorisation *ex-ante* (réglementation « R. 226 » du code pénal comme de l'article L. 34-11 du code des postes et des communications électroniques). Il conviendra d'être attentifs à ces évolutions, afin de préserver les garanties essentielles à la sécurité nationale qu'apportent aujourd'hui ces dispositions.

12. IT correspond aux infrastructures de télécommunication c'est-à-dire aux infrastructures des opérateurs de communications.

13. OTT correspond aux termes « over the top » c'est-à-dire à un service de communication ou de livraison de média sans la participation d'un opérateur de réseau traditionnel fournissant la connexion à Internet.

# Dossier 2. Les algorithmes

## Éclairage : L'algorithme : d'un concept simple à une réalité complexe

**M. Gérard Biau,**
**Professeur à Sorbonne Université, directeur de SCAI (Sorbonne Center for AI) et membre de l'Académie des sciences**

**M. Arnaud Latil,**
**Maître de conférences HDR à Sorbonne Université, membre de SCAI et du CERDI (Université de Saclay)**

Le mot algorithme tire son origine du nom du mathématicien perse du IX$^{e}$ siècle, Al-Khwârizmî. Ce dernier a écrit un ouvrage majeur intitulé « Abrégé du calcul par la restauration et la comparaison », qui est à l'origine du terme « algèbre ». Le mot algorithme est une déformation du latin médiéval algoritmi, qui désignait les procédés de calcul inspirés des travaux Al-Khwârizmî. Ce terme a été utilisé par les traducteurs latins pour nommer les méthodes de calcul et de résolution de problèmes décrits dans ses travaux, notamment celles basées sur le système de numération décimal introduit en Europe à partir du monde arabo-islamique.

Dans le langage moderne, un algorithme peut être défini de plusieurs manières selon le contexte. En informatique, il s'agit d'une suite finie d'instructions ou d'opérations logiques permettant de résoudre un problème ou d'accomplir une tâche spécifique. Plus généralement, un algorithme peut être vu comme une méthode ou un processus systématique pour atteindre un objectif donné, que ce soit dans les mathématiques, les sciences sociales ou d'autres disciplines.

Une recette de cuisine, par exemple, est un algorithme, dans la mesure où elle décrit un processus structuré et ordonné pour atteindre un objectif précis, en l'occurrence la préparation d'un plat. D'autres exemples classiques incluent l'algorithme d'Euclide, utilisé pour calculer le plus grand commun diviseur de deux nombres, ou les algorithmes de tri (comme le tri à bulles ou le tri rapide), qui permettent d'ordonner une liste d'éléments.

Dans notre quotidien, les algorithmes sont au cœur de nombreux systèmes contemporains. Les moteurs de recherche comme Google Search utilisent des algorithmes sophistiqués pour classer des milliards de pages web. Les plateformes de streaming et d'information (Netflix, Facebook, etc.) exploitent des algorithmes de recommandation pour personnaliser le fil d'actualité en fonction des préférences de chaque utilisateur. Les systèmes financiers utilisent des algorithmes de trading pour effectuer des transactions en une fraction de seconde.

À partir des années 2000, l'algorithmique connaît une profonde transformation sous l'impulsion de l'intelligence artificielle et du développement de l'apprentissage automatique (*machine learning* en anglais). Ces technologies, qui reposent pour l'essentiel sur des modèles complexes (les réseaux de neurones profonds, les architectures transformers, etc.) entraînés à partir d'immenses volumes de données, marquent une rupture avec les algorithmes traditionnels. Désormais, il ne s'agit plus seulement de règles

explicites et programmées, mais de systèmes capables d'apprendre, d'évoluer et d'adapter leurs réponses en fonction des données qu'ils ingèrent. Le développement de ces systèmes nécessite une puissance de calcul colossale, rendue possible par les progrès exponentiels dans le matériel informatique, au travers notamment des processeurs graphiques (GPU). Ces infrastructures permettent d'entraîner de grands modèles (dits de fondation), d'une complexité sans précédent, capables de traiter des données multimodales (texte, images, vidéos, etc.), d'accomplir efficacement des tâches toujours plus spectaculaires, ou de détecter des motifs invisibles à l'œil humain.

Ce nouveau paysage rend alors floue la notion d'algorithme, en la repositionnant à la frontière entre les modèles eux-mêmes, leur entraînement, le savoir-faire industriel, et les boucles de rétroaction générées par les interactions avec les utilisateurs. ChatGPT, par exemple, est-il simplement un algorithme ? Ou bien un produit industriel, façonné par des choix stratégiques, des méthodes statistiques et des données collectées ? Il illustre cette zone grise où la technologie, le savoir-faire humain et les comportements collectifs se mêlent pour produire un outil qui dépasse la somme de ses parties.

La convergence entre données, algorithmes et intelligence artificielle ouvre un champ nouveau, à la croisée de la science, de l'ingénierie et des sciences humaines. Ce nouvel écosystème soulève des questions fondamentales sur la transparence, la responsabilité et l'équilibre des pouvoirs. Qui contrôle ces systèmes, et dans quel intérêt ? Où s'arrête l'algorithme et où commence la stratégie industrielle ? Ce n'est plus seulement un enjeu technique : c'est une révolution culturelle et sociétale, où les règles du jeu sont en train d'être redéfinies.

Du point de vue des politiques publiques, les algorithmes font l'objet d'encadrements émergents, qui diffèrent suivant les pays, les

cultures et les continents. En Europe, malgré cette complexité grandissante, la régulation des algorithmes et des systèmes de traitement automatisé de données s'inscrit encore aujourd'hui dans un cadre juridique aux objectifs et aux méthodes classiques, principalement fondés sur les objectifs de transparence, d'explicabilité et de contrôle. Le droit des données à caractère personnel, le droit administratif, le droit de la santé ou encore le droit de l'intelligence artificielle prévoient ainsi des obligations d'information, parfois des obligations d'explication, lorsque des algorithmes sont mis en œuvre. Le RGPD et le récent Règlement relatif à l'IA en sont des manifestations emblématiques. Lorsque des usages algorithmiques risquent de porter plus gravement atteinte aux droits et aux libertés, le législateur déploie ensuite des procédures d'inspection ou d'audit, comme c'est le cas par exemple pour les algorithmes de modération et de recommandation de contenus utilisés par les plateformes, comme le prévoit le Digital Services Act. Dans les cas les plus gravement attentatoires aux libertés, une autorisation préalable de l'administration se trouve alors requise, comme cela est le cas concernant certaines techniques de renseignement.

Ces outils juridiques se heurtent cependant à la complexité grandissante des algorithmes, associée à l'accroissement de leur rôle dans l'économie, l'information, l'emploi ou encore l'enseignement. En réaction, une nouvelle génération d'outils juridiques prend forme. Ils s'inscrivent dans une approche dite « par les risques », consistant non seulement à moduler la fermeté de l'action législative en fonction de la gravité considérée des usages algorithmiques, mais aussi et surtout à en évaluer les conséquences sur la société. Sur le plan des méthodes législatives, le développement des lois d'expérimentation et des bacs à sable réglementaires témoigne de cette conception réaliste de la complexité algorithmique. La mise en place de scores, comme le « cyber score », ou encore d'obligations de cartographie des

risques par les opérateurs s'inscrit ainsi dans cette logique de monitoring algorithmique.

Mais il reste une catégorie de risques, encore plus sensible et vertigineuse, dont l'appréhension soulève un défi majeur pour les politiques publiques : il s'agit des risques systémiques. Cette expression désigne les risques de perturbation généralisée de l'ensemble d'un système organisé, comme le système financier, le système de santé ou encore le système démocratique. La grande crise financière de 2008 a contribué à placer les risques systémiques sur le devant de la scène : la circulation incontrôlée de « créances pourries » par la médiation de mécanismes de titrisation, ni contrôlés ni même réellement compris des pouvoirs publics, a conduit à faire chavirer l'ensemble du système financier international. Plus proche de nous, la pandémie de COVID-19 survenue en 2020, a bouleversé l'organisation économique et sociale à l'échelle mondiale, montrant ainsi l'ampleur et la puissance que peuvent revêtir les risques systémiques.

Dans ce contexte, les algorithmes se trouvent à la source d'au moins deux risques systémiques. Le premier porte sur les risques informationnels, la circulation des savoirs et des connaissances. À la faveur du développement des outils d'intelligence artificielle générative, dont ChatGPT représente le symbole, la perte de maîtrise de l'information devient un sujet central. Ce ne sont pas tant les risques d'erreurs (les fameuses « hallucinations » qui, au fond, ne sont que le reflet de la nature probabiliste des algorithmes au cœur de l'intelligence artificielle) ou la prolifération des *deep fake*, que la perte de maîtrise du fonctionnement des outils algorithmiques qui sont ici en jeu. Devenus difficilement auditables, les algorithmes d'IA, désormais incontournables, occupent une place centrale dans les décisions et la circulation l'information mondiale. Leur évolution, extrêmement rapide, dépasse la vitesse des politiques publiques.

Partiellement lié au premier, le second risque systémique porte sur les enjeux de souveraineté industrielle. La complexité des grands modèles d'intelligence artificielle, associée aux coûts de conception et d'usage, fait craindre pour la France et l'Europe une perte de contrôle de l'ensemble de la chaîne de valeur algorithmique. De la création des grands modèles à la production des GPU, en passant par la « fuite des cerveaux », le risque de décrochage économique et technologique de l'Europe est bien réel, comme l'a souligné le rapport dirigé par Mario Draghi rendu à la Commission européenne le 9 septembre 2024. Sans compter que les domaines les plus régaliens, comme la sécurité, la justice et la défense dépendent aujourd'hui étroitement des algorithmes.

Ainsi, d'objets simples, les algorithmes sont devenus des réalités complexes, tant sur le plan technique que politique. Pour l'Europe, leur régulation nécessite une véritable stratégie industrielle, qui doit aller au-delà des objectifs – légitimes et nécessaires – de confiance, de loyauté et de transparence. Relever le défi de cette complexité impose un changement d'échelle ambitieux et une réactivité sans précédent des politiques publiques. Il ne s'agit plus pour l'Europe de se contenter de suivre, mais de s'affirmer face aux nouveaux enjeux, à commencer par la révolution quantique qui se profile.

# Étude : L'algorithme au sens du code de la sécurité intérieure : d'une vision fantastique à une réalité juridique

« ***Les algorithmes sont les architectes invisibles de nos vies numériques. Il est temps qu'ils sortent de l'ombre.*** »[1] C'est en ces termes que Margrethe Vestager, vice-présidente de la Commission européenne et commissaire en charge de la concurrence jusqu'en novembre 2024, appuyait les démarches lancées par la Commission fin 2023 pour obtenir des grands moteurs de recherche en ligne et plateformes numériques (Apple, Google, Meta, TikTok, Snapchat, YouTube, Amazon, et le réseau social X), une meilleure transparence sur le fonctionnement de leurs algorithmes de recommandation de contenus.

Cette formule met en avant, au-delà de la puissance acquise par les géants du net, le rôle structurant joué par les algorithmes, et partant, par les acteurs qui les maîtrisent, dans la construction et l'animation de notre monde numérique.

Définie usuellement par les mathématiciens comme une suite d'instructions précises permettant d'aboutir à un résultat à partir de données fournies en entrée, la notion d'algorithme[2] se concrétise de fait dans la sphère numérique par des processus automatisés très divers, des plus rudimentaires, s'appuyant sur une formule mathématique aisément compréhensible par tous, aux plus complexes, dont la sophistication et l'hermétisme contribuent à leur donner l'allure de « boîtes noires ».

1. Citée dans « Le Parlement européen demande à X ses algorithmes de recommandations », S. Soarez, Innovations.fr, 17 janvier 2025. Voir également les publications de la Commission européenne relative à la procédure formelle ouverte à l'encontre de X le 18 décembre 2023 et les mesures d'enquête supplémentaires adressées le 17 janvier 2025 : https://digital-strategy.ec.europa.eu/fr/news/commission-opens-formal-proceedings-against-x-under-digital-services-act et https://digital-strategy.ec.europa.eu/fr/news/commission-addresses-additional-investigatory-measures-x-ongoing-proceedings-under-digital-services.

2. Pour une présentation du concept d'algorithme, voir la contribution de MM. Gérard Biau et Arnaud Latil « *L'algorithme : d'un concept simple à une réalité complexe* » p. 135 du présent rapport.

À l'instar des systèmes d'intelligence artificielle, avec lesquels ils sont souvent confondus, les algorithmes sont omniprésents dans le débat public[3]. Leur maîtrise est devenue une préoccupation démocratique essentielle, au point de placer ces outils au cœur des réglementations qui prennent place pour encadrer le monde numérique, en particulier au niveau européen.

L'univers du renseignement, lui aussi marqué par la prégnance des technologies numériques, n'échappe pas aux questionnements sur l'utilisation des algorithmes pour appuyer la surveillance.

Le droit du renseignement présente toutefois l'originalité d'avoir érigé cet outil mathématique en technique de renseignement à part entière, en sus de prévoir son usage pour traiter les données recueillies de la surveillance. Ainsi, l'une des techniques de renseignement dont l'emploi par les services de renseignement français est autorisé par le code de la sécurité intérieure (CSI) est un traitement automatisé, communément dénommé « algorithme », visant à permettre la détection de menaces ou d'indices de menaces à partir de l'exploitation d'une masse de données numériques.

## L'ALGORITHME DANS LA RÉGLEMENTATION EUROPÉENNE SUR LE NUMÉRIQUE : UNE ILLUSTRATION DES ENJEUX

La politique numérique de l'Union européenne (UE) comporte différents volets visant à la fois à assurer la compétitivité européenne en la matière, à réguler son marché intérieur et à préserver le respect des droits et libertés garantis notamment par la Charte des droits fondamentaux. Tenant compte de leur importance dans l'espace

3. Voir également l'éclairage consacré à l'intelligence artificielle et au renseignement par le 8ème rapport d'activité 2023 de la CNCTR, p. 135 et suivantes.

numérique, plusieurs des règles de gouvernance posées par la réglementation européenne visent spécifiquement les algorithmes.

La technique de l'algorithme, objet de la présente étude, n'est pas régie par cette réglementation dès lors que le renseignement ne relève pas du champ du droit de l'UE. Un bref survol des textes adoptés au niveau européen reste toutefois riche d'enseignement sur les enjeux que soulève la maîtrise de l'usage des algorithmes.

**La législation sur l'intelligence artificielle : *l'Artificial Intelligence Act (AI Act)*[4]**

Ce texte s'attache à promouvoir l'adoption en Europe d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance. Il encadre les systèmes d'intelligence artificielle (SIA) mis sur le marché européen afin qu'ils soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux en fixant des règles à suivre par tous les développeurs et les déployeurs d'IA, différenciées sur les risques que présente chaque système[5].

Les algorithmes sont au cœur de cette réglementation, dès lors qu'ils servent à la construction de tous les SIA complexes.

**La législation visant à réguler Internet : *le Digital Markets Act*[6] *et le Digital Services Act*[7]**

Le règlement sur les marchés numériques (*Digital Markets Act*, ou DMA) vise à lutter contre les pratiques anticoncurrentielles des géants d'internet et à corriger les déséquilibres de leur domination sur le marché numérique européen. Il encadre les activités des plus grandes plateformes, qui incluent en particulier celles des géants du

4. Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur les services numériques).

5. Voir la présentation de l'*Artificial Intelligence Act* figurant dans l'éclairage « L'Intelligence artificielle et le renseignement » au sein du 8ème rapport d'activité 2023 de la CNCTR.

6. Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques).

7. Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

net souvent présentés sous l'acronyme « GAFAM[8] », eu égard à leur rôle de « contrôleurs d'accès » à l'entrée d'internet (« *gatekeepers* »). Le règlement sur les services numériques (*Digital Services Act*, ou DSA) encadre, lui, les activités des intermédiaires numériques offrant leurs services (fournisseurs d'accès à internet, services de cloud, moteurs de recherche, plateformes de partage de contenus et de commerce, réseaux sociaux, etc.) sur le marché européen, avec pour principal objectif de faire du web un espace plus sûr pour les utilisateurs. Ce règlement prévoit des mesures visant à lutter contre la diffusion de contenus illicites et préjudiciables (incitation à la haine, désinformation, pédopornographie, etc.) ainsi que les produits et services illégaux en ligne (vente de drogues ou de contrefaçons, etc.).

Pour contrôler leur respect de cette législation, les entreprises numériques peuvent être tenues de faire la lumière sur leurs algorithmes, y compris leurs processus de recommandation de contenus. Dans son rôle de supervision et de contrôle des systèmes algorithmiques, la Commission européenne est assistée par le Centre européen pour la transparence des algorithmes (ECAT), inauguré le 18 avril 2023. Les scientifiques et experts du centre ont pour mission d'apporter leur expertise technique pour analyser les algorithmes, identifier et gérer les risques systémiques posés par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne, et étudier l'impact sociétal à long terme des algorithmes.

**La législation sur le contrôle des données : le *Data Act*, le *Data Governance Act*[9] et le RGPD[10]**

Le règlement sur la gouvernance des données (*Data Governance Act*), et le règlement sur les règles harmonisées en matière d'accès et

8. Acronyme visant Google (et le groupe Alphabet dont elle relève), Apple, Facebook (et le groupe Meta), Amazon, et Microsoft.

9. Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (règlement sur la gouvernance des données], et règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données).

10. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

d'utilisation équitables des données (*Data Act*) visent à renforcer la compétitivité et la souveraineté de l'UE dans la gouvernance des données en définissant un cadre harmonisé permettant aux acteurs économiques et aux États membres de l'UE de tirer parti du potentiel des données et de favoriser l'innovation. Ces textes ont ainsi pour objectif de promouvoir l'accès, le partage et la réutilisation des données en Europe, dans le respect du droit de l'UE – en particulier des règles de protection des données personnelles fixées par le règlement général sur la protection des données (RGDP). Ce dernier vise à permettre aux résidents européens de mieux contrôler leurs données à caractère personnel en encadrant les traitements automatisés dont elles peuvent faire l'objet. Il reprend et complète les grands principes déjà inscrits dans le droit européen et dans la loi « Informatique et libertés » du 6 janvier 1978, notamment le droit d'accès aux données personnelles, les droits de rectification et d'effacement de ses données et la possibilité de demander un déréférencement.

Dès lors qu'ils traitent ou utilisent des données, les algorithmes doivent être en conformité avec cette législation.

**La législation sur la cyber sécurité : la directive *Network and Information Security 2 (NIS 2)*[11]**

La directive sur la sécurité des réseaux et des systèmes d'Information (dite NIS 2) vise à élever le niveau global de cybersécurité en Europe par l'application d'un cadre harmonisé et simplifié fixant des règles de renforcement des mesures de cybersécurité, de gestion des incidents et de supervision des entités fournissant des services essentiels au maintien d'activités sociales ou économiques critiques. Elle est précisée et complétée par trois règlements européens : le règlement relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, dit *Cybersecurity Act*, le règlement relatif aux exigences horizontales de cybersécurité

11. Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union.

applicables aux produits comportant des éléments numériques, appelé *Cyberresilience Act* (CRA), le règlement établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir sur la cybersolidarité, ou *Cyber solidarity Act*.

La présente étude vise, dans le respect du secret de la défense nationale, à exposer la réalité juridique et technique (1). Ainsi, le spectre de l'outil d'une surveillance de masse peut être dissipé en décrivant une technique de détection de menaces rigoureusement contrôlée (2).

# 1. Du spectre de l'outil d'une surveillance de masse...

## 1.1. La genèse du cadre légal : la voie de l'expérimentation face à une technique redoutée

### 1.1.1. Une exception limitée mais nécessaire au principe de la surveillance ciblée et individualisée

Le cadre juridique posé par le livre VIII du code de la sécurité intérieure (CSI) relatif au renseignement est construit autour du principe cardinal posé par son article liminaire suivant lequel « ***Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi*** » (voir article L. 801-1).

**Pour assurer le respect de ce principe, le législateur a fait le choix de l'individualisation de la surveillance opérée sur le**

**territoire national ou visant des identifiants techniques, tels que des numéros de téléphone ou des adresses électroniques, rattachables au territoire national.** En effet, les techniques de renseignement prévues par la loi dans ce champ renvoient à des outils destinés à mettre sous surveillance un individu déterminé ou ses attributs (véhicule, domicile, identifiants, correspondances ou paroles, etc.). Corrélativement, l'article L. 821-2 du CSI impose que lorsqu'un service de renseignement sollicite la mise en œuvre d'une technique de renseignement, il doit préciser, outre les finalités et motifs de la surveillance, la ou les personnes concernées par la technique. Cette personne peut, certes, être identifiée ou non, relever, pour certaines techniques, de l'entourage[12] de la cible principale, voire, dans de rares situations particulièrement contrôlées par la commission, être une personne morale ou une entité de fait, sans personnalité juridique. Il n'en demeure pas moins que l'ensemble de l'édifice juridique du droit du renseignement français est construit autour d'une mise en œuvre individualisée et ciblée des techniques de surveillance domestique, à rebours du choix de la surveillance de masse retenue par certains Etats.

Application fondamentale et structurante du principe de proportionnalité de la surveillance posé par le législateur de 2015, l'individualisation des techniques de renseignement reflète le choix d'un recueil d'informations limité au strict nécessaire. Cette approche s'oppose notamment, à l'option américaine qui permet aux services de renseignement d'intercepter et de stocker

12. Voir sur ce point la fiche thématique « *L'entourage des personnes surveillées* » disponibles sur le site internet de la CNCTR ainsi que l'étude « *Surveiller l'entourage ?* » dans le 8ème rapport d'activité 2023 de la CNCTR, p. 117 et suivantes.

massivement les données de ses résidents et non-résidents[13], dont la pratique extensive a été mise au jour en juin 2013 par les révélations d'Edward Snowden, ancien consultant de la *National Security Agency* (NSA), sur l'existence de programmes de collecte systématique des métadonnées des appels téléphoniques passés aux États-Unis ou depuis les États-Unis vers l'étranger. Ainsi qu'il ressort des débats parlementaires de l'époque, **le législateur français a entendu écarter fermement l'instauration d'une « *surveillance indifférenciée de masse* »** par les services de renseignement qui pourrait s'exercer, comme aux Etats-Unis, ***« sans autre réelle restriction que celle induite par les limites technologiques »***, différence de choix illustrée par l'image de la « pêche au harpon » française opposée à la « pêche au chalut » américaine.

13. La surveillance de masse aux États-Unis : du programme USTO au *Patriot Act*.

Le programme USTO : le programme « *US to other countries* », dit « USTO, mis en place en 1992, est souvent présenté comme le premier programme américain de surveillance de masse des télécommunications. Il imposait à tous les opérateurs téléphoniques de fournir la liste de tous les appels depuis les États-Unis vers des pays qui seraient susceptibles de participer à des trafics de drogue.

Dans de le cadre de ce programme, avalisé par le Département de la justice américain, une surveillance des communications des citoyens américains et des ressortissants de 116 pays aurait été mise en place au profit de la *Drug Enforcement Administration* (DEA), agence en charge de la lutte contre le trafic de drogue. Il a été officiellement mis fin à ce programme en 2013, à la suite des révélations d'Edward Snowden.

Le FISA et le *Patriot Act* :

Depuis l'après-guerre, et singulièrement dans le contexte de la guerre froide, les Etats-Unis n'ont cessé de développer leurs capacités d'interception des communications, notamment dans le cadre des partenariats de renseignement entre alliés d'après-guerre.

En termes d'exploitation, les systèmes de surveillance américains ont été nettement renforcés à la suite des attentats du 11 septembre 2001, avec, en particulier, l'adoption le mois suivant du *USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)*, loi qui a étendu les prérogatives de la National Security Administration (NSA), et des autres agences de renseignement et d'investigation (FBI et CIA en particulier) en facilitant la réquisition des données en matière de surveillance domestique. Les agences disposent désormais de plus larges pouvoirs pour récupérer auprès des opérateurs de télécommunication les informations personnelles des usagers et archiver et exploiter des masses de données issues de la surveillance électronique, dans un cadre préventif. Quelques années plus tard, une nouvelle disposition adoptée en 2008 est venu en outre légaliser des techniques de surveillance autorisées secrètement par la Maison Blanche après les attentats. La section 702 du *Foreign and Intelligence Act* (FISA) de 1978 FISA autorise depuis les agences de renseignement à collecter largement les données de citoyens et d'entreprises situés en dehors du territoire des Etats-Unis, donnant aux dispositifs de surveillance américains un champ d'application particulièrement large.

Si une partie des régimes d'exception adoptés en réaction aux attentats de 2001 ont été revus ou supprimés, notamment le très controversé programme de stockage et d'exploitation des métadonnées téléphoniques et informatiques des Américains autorisé dans un cadre préventif par la section 215 du *Patriot Act*, l'essentiel des dispositifs de surveillance de masse, domestique et internationale, restent durablement ancrés dans le paysage législatif américain.

Voir notamment le rapport n° 2697 du 2 avril 2015 de M. Jean-Jacques Urvoas au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de l'Assemblée nationale, et l'audition des ministres à l'Assemblée nationale le 31 mars 2015.

En France, seule la surveillance des communications électroniques internationales, lorsqu'elle n'a pas pour objet le suivi d'identifiants rattachables au territoire national, échappe à cette règle. La différence d'approche par rapport à la surveillance domestique tient au fait que, dès lors que des personnes situées à l'étranger échappent à la juridiction de l'État, et ne peuvent en particulier faire l'objet de mesures juridiques contraignantes qui se fonderaient sur les éléments collectés, l'interception de leurs communications n'est pas susceptible de porter atteinte à leurs droits dans la même mesure que si elles se situaient sur le territoire national[14].

## LA SPÉCIFICITÉ DE LA SURVEILLANCE INTERNATIONALE

Malgré l'effacement des frontières physiques dans le monde numérique, le droit du renseignement reste marqué par le principe de territorialité.

La surveillance des communications électroniques internationales, qu'elle porte sur des correspondances ou des données de connexion, est ainsi régie par un chapitre spécifique du titre V du livre VIII relatif au renseignement du code de la sécurité intérieure.

Les dispositions des articles L. 854-1 à L. 854-9 du CSI, qui constituent ce chapitre, prévoient que les services de renseignement peuvent être autorisés à exploiter les communications émises ou reçues à l'étranger sur les réseaux de communications électroniques désignés par le Premier ministre. À la différence des techniques mises en œuvre sur le territoire national ou portant sur un identifiant technique rattachable au territoire national, qui relèvent d'une surveillance individualisée et ciblée, les communications électroniques internationales peuvent être surveillées au moyen d'autorisations non individualisées, visant des zones géographiques, des organisations, ou des groupes (voir le 3° du III de l'article L. 854-2).[15]

14. Voir les observations du Gouvernement sur la décision n° 2015-722 DC du 26 novembre 2015 du Conseil constitutionnel et l'étude du Conseil d'État « *Le numérique et les droits fondamentaux* » - 2014.

15. Voir sur ce point la présentation « La surveillance des communications électroniques internationales » disponible sur le site internet de la CNCTR.

**La nécessité de donner aux services les moyens d'action adéquats et proportionnés aux menaces à prévenir a conduit à l'introduction d'une exception au principe de la surveillance ciblée et individualisée.**

Deux contraintes majeures ont conduit le législateur à admettre une entorse à ce principe.

L'intensification et la diversification de la menace depuis le début du siècle, marquée en particulier par le développement d'une mouvance terroriste aux ramifications mondiales comprenant une myriade de cellules et d'individus isolés, ont rendu nécessaire le recours à des procédés de surveillance à même de détecter cette menace disséminée et protéiforme, constituée entre autres par des individus sans contact apparent avec des organisations ou réseaux ou groupes structurés.

Ensuite, la croissance exponentielle de la production de données, qui a accompagné l'essor des technologies numériques, comme le développement des réseaux d'échanges sécurisés, ont montré les limites des outils de surveillance historiques, impuissants à repérer les infractions et menaces dans le flot massif et permanent de données circulant dans l'espace numérique.

Conscient de ces enjeux, le législateur a souhaité ouvrir la possibilité, pour les services de renseignement français, de mettre en place un traitement algorithmique aux fins de détecter une menace terroriste, sans pour autant procéder à l'identification des personnes concernées par l'analyse des données autres que celles suspectées de terrorisme. L'objectif poursuivi était donc de recouper et analyser un grand nombre d'éléments techniques en vue de détecter des signaux de faible intensité suggérant une menace terroriste, sans pour autant verser dans une surveillance de masse c'est-à-dire en ne concédant aucune « atteinte collatérale » aux libertés individuelles.

Il est essentiel de préciser que le lot de données sur lequel s'exécute l'algorithme n'est pas mis à disposition des services, seules les quelques portions associées aux résultats positifs de détection le sont.

### 1.1.2. L'instauration à titre expérimental de la technique algorithmique par la loi du 24 juillet 2015

**La loi du 24 juillet 2015 relative au renseignement a consacré une utilisation spécifique des algorithmes, technique de renseignement à part entière, pour les seuls besoins de la prévention du terrorisme.** Pour ce faire, son article 5, repris à l'article L. 851-3 du code de la sécurité intérieure, a autorisé la mise en œuvre de techniques de traitement algorithmique, couramment désignées sous le vocable d'« algorithmes », sur les données des opérateurs de communications électroniques et des fournisseurs de services internet en vue de détecter des connexions susceptibles de révéler une menace terroriste.

Les algorithmes régis par l'article L. 851-3 du CSI sont ainsi devenus en 2015 la seconde catégorie de traitements algorithmiques autorisés par la loi sur des données de masse en matière de sécurité publique, aux côtés de ceux instaurés en 2013 pour l'analyse des données à caractère personnel recueillies à l'occasion de déplacements internationaux, prévus par l'article L. 232-7 du même code[16].

16. Système API-PNR portant sur les données d'enregistrement et de réservation des passagers.

## UNE TECHNIQUE DE RENSEIGNEMENT VALIDÉE PAR LE CONSEIL CONSTITUTIONNEL

Saisi de la loi relative au renseignement, le Conseil constitutionnel a déclaré conformes à la constitution les dispositions de l'article L. 851-3 du code de la sécurité intérieure sur les traitements algorithmiques[17], jugeant qu'elles ne portaient pas une atteinte manifestement disproportionnée au droit au respect de la vie privée.

Il a relevé en particulier que « *tant le recours à la technique que les paramètres du traitement automatisé sont autorisés après avis de la commission nationale de contrôle des techniques de renseignement* », que les traitements automatisés, destinés à révéler une menace terroriste, utiliseront exclusivement des données de connexions « *sans recueillir d'autres données que celles répondant à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent* » et enfin que, « *lorsqu'une donnée détectée par le traitement automatisé est susceptible de caractériser l'existence d'une menace terroriste, une nouvelle autorisation du Premier ministre sera nécessaire, après avis de la commission nationale de contrôle des techniques de renseignement, afin d'identifier la personne concernée (…)* ».

**Signe de sa vigilance vis-à-vis de ce nouvel outil de surveillance, novateur et complexe, le législateur a fait le choix d'un dispositif expérimental, son emploi n'étant prévu que pour trois ans, jusqu'au 31 décembre 2018.**

Cette date a toutefois été reportée à deux reprises, prolongeant l'expérimentation jusqu'au 31 décembre 2021.

Une première prolongation s'est imposée en raison des difficultés rencontrées dans la mise au point de la technique nouvelle de l'algorithme, conjuguées au contrôle rigoureux exercé par la CNCTR sur cette expérimentation. Après une phase d'études et d'examen des options possibles menées par le Groupement

17. Voir la décision n° 2015-713 DC du 23 juillet 2015 du Conseil constitutionnel, §58 et suivants.

interministériel de contrôle (GIC), en liaison avec la Direction générale de la sécurité intérieure (DGSI) et la Direction générale de la sécurité extérieure (DGSE), le projet d'architecture générale retenu pour la mise en œuvre des traitements automatisés n'a été arrêté qu'au printemps 2017 par une décision classifiée du Premier ministre du 27 avril, les premières ébauches ayant été révisées pour tenir compte des observations et recommandations formulées par la CNCTR concernant, en particulier, les conditions stockage et d'accès aux données[18]. Après validation du cadre technique général, des études supplémentaires ont été nécessaires pour construire le premier algorithme, en particulier pour déterminer les paramètres d'alerte susceptibles d'être l'indice d'une menace terroriste et choisir les données traitées afin de construire un dispositif opérationnel, pertinent et proportionné. La complexité de ces travaux préparatoires explique que la première mise en œuvre d'un d'algorithme n'ait finalement été autorisée par le Premier ministre que le 12 octobre 2017[19], après des avis favorables émis par la formation plénière de la CNCTR par deux délibérations classifiées des 26 juillet et 5 octobre 2017.

Face au peu de recul qu'aurait laissé l'échéance initialement retenue pour évaluer les apports opérationnels des algorithmes, mis en service effectivement à partir de la fin de l'année 2017, l'expérimentation a été prolongée jusqu'au 31 décembre 2020 par l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, dite loi SILT.

Une seconde prolongation du délai d'expérimentation a été décidée par l'article 2 de la loi n° 2020-1671 du 24 décembre 2020 pour tenir compte de l'impact de la crise sanitaire résultant de l'épidémie de Covid-19 sur le travail gouvernemental et le calendrier parlementaire, de nature à rendre difficile l'examen par le

18. Pour une description détaillée de la conception de l'architecture technique des algorithmes, voir le 2ème rapport d'activité 2017 de la CNCTR, p. 16 et suivantes.

19. Voir le rapport d'activité 2020 de la CNCTR, p. 16 et suivantes.

Parlement, en temps utile et dans des conditions de débat appropriées, du choix de la pérennisation ou de la suppression du nouvel outil de surveillance fondé sur les traitements automatisés.

## Un autre exemple des réserves suscitées par l'usage des algorithmes en matière d'ordre public mais en dehors du champ de compétence des services de renseignement : la vidéosurveillance dite « augmentée » ou « intelligente »

**Intervenant hors du champ de compétence des services de renseignement**, le déploiement dans les lieux ouverts au public des dispositifs de caméra ou de vidéo « augmentée », c'est-à-dire de dispositifs de captation d'images auxquels sont associés des logiciels de traitements algorithmiques permettant une analyse automatique des données captées afin, par exemple, de détecter des formes ou des objets, d'analyser des mouvements, ou repérer des comportements contraires à l'ordre public ou des infractions, a suscité de vifs débats ces dernières années.

Les nouveaux enjeux soulevés par l'utilisation de plus en plus courante des techniques vidéo s'appuyant sur l'intelligence artificielle, notamment par des autorités publiques dans le cadre de projets dits de *safe city*, lancés à Nice, Marseille ou Saint-Etienne, ont été mis en avant par des autorités administratives indépendantes, des associations ou encore des universitaires, appelant un encadrement étroit des différents usages. La Commission nationale de l'informatique et des libertés (CNIL), notamment, a souligné le changement de nature de la vidéosurveillance algorithmique par rapport aux caméras classiques filmant en direct et enregistrant des séquences vidéo visionnées par un opérateur humain. La démultiplication des capacités du dispositif et le traitement massif de données à caractère personnel présentent un risque particulier pour

les droits et libertés individuels et collectifs, conduisant à un risque accentué de surveillance généralisée[20].

L'usage le plus controversé de ces dispositifs est sans doute celui de la vidéosurveillance algorithmique en matière de sécurité publique. En témoignent les débats parlementaires qui ont précédé l'adoption de l'article 10 de la loi n° 2023-380 relative aux Jeux olympiques et paralympiques de 2024, autorisant à titre expérimental l'utilisation de la vidéosurveillance augmentée au moyen de caméras fixes ou de drones pour la sécurisation de manifestations sportives, récréatives et culturelles.

Comme pour la technique de l'algorithme prévue à l'article L. 851-3 du CSI, le législateur a retenu une approche prudente, fondée sur une expérimentation, l'utilisation de la vidéosurveillance algorithmique n'étant autorisée que jusqu'au 31 mars 2025. Il a par ailleurs étroitement encadré l'emploi de cet outil dans ses finalités comme dans ses conditions de mises en œuvre, n'autorisant que la détection d'anomalies ou de situations à risque limitativement déterminées, et bannissant l'usage de tout procédé de nature à permettre l'identification d'une personne physique.

Le rapport du comité d'évaluation sur cette expérimentation[21], remis en janvier 2025 au Parlement et à la CNIL, met en avant les apports de la vidéosurveillance algorithmique en matière de sécurité et expose les réticences et craintes du public comme des organismes investis dans la défense des droits et libertés, notamment sur l'effet de cliquet de l'adoption d'une nouvelle technologie plus intrusive, qui pourrait banaliser une surveillance générale s'appuyant sur l'IA.

20. Voir notamment la position de la CNIL sur les caméras dites intelligentes ou augmentées dans les espaces publics, publiée le 19 juillet 2022.

21. Rapport du comité d'évaluation sur l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéo protection.

## 1.2. La pérennisation et l'extension de la technique reconnues nécessaires, mais prudemment admises

### 1.2.1. Les apports indéniables de la technique ont conduit à sa pérennisation, assortie toutefois de nouvelles garanties

Sans attendre l'échéance laissée au gouvernement pour adresser au Parlement un rapport sur l'expérimentation de la technique de l'algorithme, fixée en dernier lieu au 30 juin 2021, plusieurs acteurs de la politique publique du renseignement se sont prononcés sur les apports des traitements automatisés mis en œuvre.

Mettant en avant la menace terroriste, les rapporteurs de la mission d'information de l'Assemblée nationale sur l'évaluation de la loi du 24 juillet 2015[22] ont souligné, dès l'été 2020, la nécessité de proroger l'emploi de l'algorithme, cette technique répondant à leurs yeux à un besoin opérationnel. Malgré une mise en œuvre relativement limitée, trois traitements algorithmiques seulement ayant été mis en œuvre et en fonctionnement début 2020, la mission concluait à des résultats intéressants et évoquait même des pistes de réflexion afin d'améliorer l'efficacité d'un dispositif déjà prometteur.

De même, la CNCTR s'est prononcée en faveur de la poursuite de la surveillance par algorithme, justifiée par la réalité d'une menace terroriste persistante et diffuse. Elle a reconnu l'apport de cet outil de détection, seul à même dans l'arsenal des techniques autorisées

22. Voir rapport d'information n°3069 déposé le 10 juin 2020 par la mission commune d'information de la commission des lois/commission de la défense de l'Assemblée nationale sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement et présenté par M. Guillaume Larrivé, Président, MM. Loïc Kervran et Jean-Michel Mis, rapporteurs.

par le code de la sécurité intérieure, de repérer des profils d'individus isolés dont le potentiel dangereux ne peut parfois être révélé qu'à travers leur activité numérique[23]. Le bilan d'emploi de la technique, développé dans un rapport classifié du gouvernement du 30 juin 2020 à destination de la délégation parlementaire au renseignement (DPR) et de la commission, lui est apparu suffisamment convaincant pour préconiser la pérennisation du dispositif de l'article L. 851-3 du CSI, à l'expérimentation duquel elle a été étroitement associée[24]

Sans exposer les éléments de ce rapport, couverts par le secret de la défense nationale, le gouvernement a présenté dans l'étude d'impact du 11 mai 2021, relative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement proposant la pérennisation des dispositions relatives à l'algorithme, des informations générales sur le déroulement de l'expérimentation et l'efficacité opérationnelle de la technique. Sur ce dernier point, l'étude indique que le dispositif « ***s'avère indispensable pour permettre de détecter des individus inconnus des services de renseignement ou que leurs comportements antérieurs n'avaient jusqu'ici pas permis d'identifier comme menaçants*** », précisant que les algorithmes en fonctionnement ont notamment permis « ***d'identifier des individus porteurs d'une menace à caractère terroriste et de détecter des contacts entre les individus porteurs de menace ; d'obtenir des informations sur la localisation d'individus en lien avec cette menace ; de mettre à jour des comportements d'individus connus des services de renseignement et nécessitant des investigations plus approfondies ; d'améliorer la connaissance des services sur la manière de procéder des individus de la mouvance terroriste*** ». Le gouvernement a conclu

23. Voir délibération de la CNCTR n° 2/2021 du 7 avril 2021, consultable sur le site internet. https://cms.cnctr.fr/uploads/NP_CNCTR_2021_deliberation_2_2021_04_07_d5f3cf8590.pdf?updated_at=2023-04-21T16:27:30.844Z

24. Voir compte-rendu de l'audition à huis clos le mercredi 12 mai 2021 devant la Commission de la défense nationale et des forces armées de l'Assemblée nationale de M. Francis Delon, président de la CNCTR.

que la technique de l'algorithme répond à un besoin essentiel de détection précoce de la menace terroriste, en relevant, d'une part, qu'elle permet de déceler « ***une nouvelle menace, dont les auteurs et les modes opératoires ne sont pas connus et ne peuvent par définition faire l'objet d'une surveillance ciblée a priori*** », et d'autre part, qu'elle est un outil adapté au développement des nouveaux comportements numériques, « ***à la faveur notamment de la diffusion informatique d'une vaste propagande terroriste et de l'émergence de nouveaux moyens de communication électroniques***[25] ».

Au vu de ces éléments, la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, dite loi « PATR », a pérennisé la technique de l'algorithme. Néanmoins, soucieux de contenir son emploi et d'en limiter le potentiel attentatoire aux droits et libertés, le législateur a assorti cette pérennisation de nouvelles garanties, tenant essentiellement à la limitation des services de renseignement susceptibles de solliciter sa mise en œuvre et à l'habilitation exclusive du GIC pour exécuter, à la demande des services, les traitements autorisés (voir ci-dessous point 2.1.2). En outre, la loi a modifié le régime des demandes d'autorisation de mise en œuvre des techniques de renseignement, dont celle de l'algorithme, en donnant à l'avis préalable de la CNCTR un caractère très contraignant[26], assurant ainsi la mise en conformité des demandes aux exigences du droit de l'Union européenne.

### 1.2.2. … et à une extension prudente de son champ d'emploi

Autre signe de l'intérêt suscité par l'algorithme, la technique a vu son champ étendu, d'abord pour ce qui est des données susceptibles de faire l'objet d'un traitement automatisé dans la

25. Exposé des motifs du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.
26. Voir les dispositions de par l'article L. 821-1 du CSI dans sa rédaction issue de l'article 18 de la loi du 30 juillet 2021.

foulée de sa pérennisation, puis ultérieurement s'agissant des finalités invocables pour fonder sa mise en œuvre.

**Initialement cantonnés au traitement des seules données de connexion, la nécessité d'étendre les algorithmes aux adresses complètes de ressources utilisées sur internet ou URL[27] a été évoquée** dans les deux rapports précités établis en juin 2020. Le champ trop restreint des données susceptibles d'être analysées dans le cadre de l'expérimentation des traitements automatisés a en effet été jugé en partie responsable des résultats encore limités de l'outil.

L'évolution de la menace terroriste, incarnée aussi désormais par une myriade d'individus s'inspirant des messages de propagande djihadiste ou d'incitations au passage à l'acte d'organisations terroristes ou groupuscules radicalisés diffusés sur internet, rend en effet particulièrement utile, d'un point de vue opérationnel, le recueil d'URL permettant de repérer avec une précision accrue les activités numériques tenant à la consultation de sites relayant ce type de contenus.

L'élargissement de la technique de l'algorithme à l'analyse de la totalité des informations contenues dans les URL, qui revient, de fait, à autoriser un traitement automatisé de données reflétant, pour partie, le contenu de communications est donc apparu nécessaire aux services en charge de la lutte anti-terroriste.

La reconnaissance de ce besoin opérationnel par les différentes autorités publiques en charge du renseignement, notamment la CNCTR[28], a amené à ouvrir le champ des données susceptibles d'être analysées par la technique de l'algorithme aux adresses complètes de ressources utilisées sur internet, comme le précise

27. Voir encadré ci-dessous, p 160.

28. Voir la délibération n° 2/2021 du 7 avril 2021 de la CNCTR, disponible sur son site internet.

désormais l'article L. 851-3 du code de la sécurité intérieure depuis l'entrée en vigueur de la loi PATR précitée.

Là encore, l'approche prudente du législateur sur cette évolution significative de la technique s'est traduite par l'obligation faite au gouvernement d'adresser au Parlement un rapport sur l'application de l'article L. 851-3 du CSI, au plus tard le 31 juillet 2024[29], en vue de s'assurer que l'atteinte portée à la vie privée soit effectivement justifiée par une meilleure protection contre le risque terroriste. Cet élargissement du champ d'investigation de la technique s'est aussi accompagné d'aménagements du régime des données pour limiter la conservation des données traitées au strict nécessaire (voir point 2.1.2. ci-dessous).

## DONNÉES DE CONNEXION, DONNÉES DE CONTENU, ADRESSES URL

En matière de traitement des données numériques, le code de la sécurité intérieure distingue les données de connexion des données de contenu. Ainsi, son article R. 851-5 liste les données de connexion susceptibles d'être recueillies, précisant que les informations et documents concernés le sont, « *à l'exclusion du contenu des correspondances échangées ou des informations consultées (...)* ». Cette distinction rejoint celle posée par l'article L. 34-1 du code des postes et des communications électroniques, qui fixe les données relatives aux communications électroniques que les opérateurs sont tenus de conserver, précisant que lesdites données « *portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux [mais] ne peuvent en aucun cas porter sur le contenu des*

29. Cette obligation est posée au II de l'article 15 de la loi PATR précitée du 30 juillet 2021.

*correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.* »

Les données de connexion, par opposition au contenu de correspondances échangées ou d'informations consultées, désignent le « contenant », c'est-à-dire les données permettant l'acheminement d'une communication électronique.

La qualification à retenir n'est toutefois pas évidente pour certains éléments techniques tels que les adresses des sites ou pages internet, dites URL. L'URL, acronyme d'*Uniform Resource Locator*, est une chaîne de caractères alphanumériques qui précise la localisation d'une ressource internet en indiquant le type de protocole à utiliser pour accéder à la ressource (http ou https pour une page web). Son emplacement, qui correspond au nom de domaine du serveur ou à son adresse IP, le chemin d'accès à cette ressource, précise la page que souhaite consulter l'utilisateur, et le cas échéant, d'autres données complétant sa requête. Elle désigne ainsi l'adresse d'un contenu, sans pour autant constituer ce contenu.

Pour la CNCTR comme pour la CNIL[30], les URL constituent des « données mixtes », comprenant à la fois des données de connexion, pour ce qui est des éléments relatifs à l'acheminement de la communication internet, et des données de contenu, pour ce qui concerne les éléments fournissant des précisions sur l'objet ou le contenu du site internet consulté. Se fondant sur cette double nature des adresses URL, la CNCTR a considéré que les accès administratifs aux données de connexion prévus par l'article L. 851-1 du CSI ne pouvaient permettre, s'agissant des URL, que le seul recueil des parties d'URL déterminant le chemin utilisé pour échanger des correspondances ou consulter des informations, les autres éléments devant être éliminés[31].

30. Délibération CNIL n° 2015-455 du 17 décembre 2015 portant avis sur un projet de décret en Conseil d'État relatif aux techniques de recueil de renseignement (saisine n° 15033364).

31. Délibération n° 1/2016 du 14 janvier 2016 sur les modalités d'application de l'article L. 851-1 du code de la sécurité intérieure, disponible sur le site internet de la CNCTR.

La loi PATR du 30 juillet 2021 précitée consacre la nature mixte des adresses URL, regardées comme une catégorie *sui generis* de données. Depuis son adoption, le code de la sécurité intérieure précise ainsi que les techniques concernées prévues aux articles L. 851-2 (accès aux données techniques de connexion en temps réel) et L. 851-3 (algorithme) peuvent porter non seulement sur les données de connexion visées à l'article L. 851-1 mais aussi sur « les adresses complètes de ressources sur internet ».

**Par ailleurs, l'algorithme a vu le champ de son usage étendu à deux nouvelles finalités.**

Dès les premiers résultats de l'expérimentation de la technique, des voix se sont élevées pour préconiser une extension de son utilisation à d'autres finalités que la seule prévention du terrorisme, évoquant notamment l'utilité que présenterait cet outil en matière de cyberdéfense, de contre-espionnage ou plus récemment de criminalité organisée[32]. À la lumière des résultats exposés en matière de prévention du terrorisme, l'utilité de la technique pour détecter, par exemple, des manœuvres de services étrangers ou des attaques malveillantes, a ainsi pu être mise en avant.

Prenant acte de ces préconisations s'agissant du contre-espionnage et de la contre-ingérence, la loi n° 2024-850 du 25 juillet 2024 relative à la prévention des ingérences étrangères et des menaces pour la défense nationale a autorisé l'emploi de l'algorithme pour défendre et promouvoir l'indépendance nationale, l'intégrité du territoire et la défense nationale (finalité mentionnée au 1° de l'article L. 811-3 du CSI) ainsi que les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère (finalité mentionnée au 2° du même article L. 811-3) aux fins de « ***révéler des ingérences étrangères*** » et des « ***menaces pour la défense nationale*** ».

32. Voir le rapport d'information n°3069 déposé le 10 juin 2020 par la mission commune d'information de la commission des lois/commission de la défense de l'Assemblée nationale sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement et présenté par M. Guillaume Larrivé, Président, MM. Loïc Kervran et Jean-Michel Mis, rapporteurs, ainsi que le rapport d'activité de la délégation parlementaire au renseignement pour l'année 2022-20223, préconisant l'extension de l'algorithme aux finalités mentionnées au 1° et au 2° de l'article L. 811-3 du CSI à titre expérimental.

Néanmoins, renouvelant son approche prudente, le législateur n'a autorisé l'extension de l'algorithme à ces nouvelles finalités qu'à titre expérimental, pour une durée de trois ans, jusqu'au 1er juillet 2028, délai laissé aux services pour démontrer l'apport réel de la technique pour renforcer les capacités de détection de toute forme d'ingérence étrangère ou de toute menace sur la défense nationale[33].

De plus, un contrôle parlementaire renforcé sur cette nouvelle expérimentation a été mis en place par le III de l'article 6 de la loi, imposant la remise par le gouvernement de deux rapports. Un premier rapport d'évaluation devra ainsi être transmis au plus tard le 1er juillet 2026 puis un second rapport sur le bilan des résultats de la technique pour les nouvelles finalités fixées devra être fait au Parlement au plus tard six mois avant l'échéance de l'expérimentation. Ces deux rapports doivent aussi être transmis à la délégation parlementaire au renseignement (DPR) dans une version classifiée comportant les exemples de mise en œuvre des algorithmes.



33. La loi visant à sortir la France du piège du narcotrafic, adoptée les 28 et 29 avril par le Parlement, comporte toutefois une disposition visant à reporter cette date au 31 décembre 2028. Ce texte a fait l'objet de trois saisines du Conseil constitutionnel le 12 mai 2025. À la date de finalisation du présent rapport, la décision du Conseil constitutionnel n'est pas encore intervenue.

## UNE NOUVELLE EXTENSION DES FINALITÉS DE L'ALGORITHME ? LA PROPOSITION DE LOI VISANT À SORTIR LA FRANCE DU PIÈGE DU NARCOTRAFIC :

Déposé le 7 mai 2024, le rapport n° 588 « *Un nécessaire sursaut : sortir du piège du narcotrafic* » de la commission d'enquête sénatoriale présidée par M. Jérôme DURAIN préconise, au vu de l'impact du narcotrafic sur la France, « *un traitement de choc pour mettre fin à l'impunité dont jouissent les trafiquants du haut du spectre (…) et pour redonner à chaque acteur son juste rôle dans la lutte contre le narcotrafic* ». Dans cette optique, le rapport se penche sur les potentialités du renseignement algorithmique, proposant d'envisager l'extension de cette technique de renseignement à la lutte contre le narcotrafic dans un cadre expérimental *ad hoc* fixant précisément les cas de criminalité organisée justifiant son utilisation (recommandation n° 20).

S'appuyant notamment sur ce rapport, la proposition de loi visant à sortir la France du piège du narcotrafic, déposée le 12 juillet 2024 au Sénat, entend doter les services en charge de la prévention de la délinquance et de la criminalité organisées de moyens nouveaux pour suivre des narco trafiquants rompus à déjouer les capacités de surveillance classiques.

Dans sa version adoptée les 28 et 29 avril 2025 par le Parlement, le texte prévoit ainsi d'étendre l'expérimentation de l'extension de l'algorithme, prévue par la loi du 25 juillet 2024, à la finalité mentionnée au 6° de l'article L. 811-3 du CSI, et reporte par ailleurs son échéance au 31 décembre 2028[34].

34. Le texte adopté par le Parlement a fait l'objet de trois saisines du Conseil constitutionnel. A la date de finalisation du présent rapport, la décision du Conseil constitutionnel n'est pas encore intervenue.

# 2. ...à la mise en place d'une technique de détection des menaces, rigoureusement contrôlée

## 2.1. L'encadrement étroit d'une technique de détection de la menace

### 2.1.1. Les principes de fonctionnement de l'algorithme : l'articulation entre détection et surveillance, une autorisation à chaque étape

Pour présenter les traitements automatisés mis en place par la loi du 24 juillet 2015, les rapporteurs de la mission commune d'information des commissions des lois et de la défense de l'Assemblée nationale sur l'évaluation de cette loi invitaient à « ***démythifier l'algorithme*** [qui] ***n'est pas un outil de surveillance de masse, mais de détection de signaux faibles, qui pourra ensuite justifier l'usage d'une technique de renseignement, dans le cadre du droit commun*** »[35].

Dans l'architecture retenue par le législateur français, l'algorithme a en effet été conçu comme un instrument permettant la détection, en fonction de paramètres déterminés et soumis à un contrôle préalable, de signaux faibles susceptibles de révéler une menace pour les intérêts fondamentaux de la Nation, en minimisant les atteintes aux libertés individuelles. Ainsi, la technique ne permet en

35. Voir rapport d'information n°3069 déposé le 10 juin 2020 par la mission commune d'information de la commission des lois/commission de la défense de l'Assemblée nationale sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement et présenté par M. Guillaume Larrivé, Président, MM. Loïc Kervran et Jean-Michel Mis, rapporteurs.

aucune façon aux services de renseignement d'accéder à l'ensemble des données des réseaux des opérateurs et de les analyser. Au contraire, le dispositif vise à discriminer de manière la plus fine possible, parmi ces données, celles qui sont de nature à révéler une menace, afin d'orienter la surveillance des services et permettre, le cas échéant, la mise en place d'un suivi ciblé et individuel limité au strict nécessaire.

**Cette technique de renseignement fonctionne en deux temps**. Dans un premier temps, le traitement algorithmique analyse des flux de données en fonction de paramètres préétablis au moment de sa conception en vue de détecter une activité suspecte au regard de la finalité visée, sans qu'il soit possible pour les services de renseignement d'accéder directement à ces flux. Ce n'est que si, et seulement si, le traitement algorithmique détecte une activité répondant à ses critères de conception (« *hit* »), que les services de renseignement sont alertés et peuvent, dans un second temps, accéder aux seules données correspondant à ce « *hit* » ainsi qu'à l'identification des personnes auxquelles elles se rapportent, en formulant une demande de levée d'anonymisation.

La procédure mise en place peut se résumer ainsi : après que le service demandeur a obtenu l'autorisation de détecter au moyen d'un algorithme des connexions susceptibles de révéler une menace, les traitements automatisés correspondant sont mis en œuvre par le GIC. Lorsque ces traitements déclenchent une alerte, le GIC notifie ce « *hit* » au service bénéficiaire de l'autorisation de mise en œuvre de l'algorithme, sans que ce signalement ne contienne ni ne révèle les données qui l'ont déclenché. Au vu de cette information minimale, le service peut demander d'accéder aux données à l'origine de l'alerte ainsi qu'à l'identification des personnes concernées au moyen d'une demande de levée d'anonymisation, soumise à l'avis préalable de la CNCTR puis à l'autorisation du Premier ministre.

Si cette autorisation est obtenue, le GIC réunit les données et les communique au service. Ainsi, aucun service de renseignement ne peut accéder aux données soumises aux traitements automatisés. Les seules données susceptibles de leur être transmises sont celles qui ont donné lieu à une alerte de la part d'un algorithme autorisé par une première décision du Premier ministre, puis dont l'anonymat est levé par une nouvelle décision du Premier ministre.

**Trois étapes sont donc nécessaires pour que la technique algorithmique débouche sur la surveillance d'un individu**, requérant chacune une autorisation du Premier ministre, qui se prononce après avis de la CNCTR sur la demande motivée du service de renseignement concerné :

- une première autorisation pour mettre en œuvre un traitement automatisé, prononcée en application du I de l'article L. 851-3 du CSI,

- une deuxième autorisation pour obtenir la levée de l'anonymat de la personne détectée par le traitement, prononcée en application du IV du même article,

- enfin, le cas échéant, une autorisation pour recourir à une technique de renseignement visant cette personne (obtention des données de connexion ; interception de sécurité ; etc.).

La technique algorithmique prévue par le code de la sécurité intérieure ne peut ainsi être assimilée, ni dans sa finalité, ni dans sa construction, ni dans son fonctionnement légal, à un instrument de surveillance générale des informations ou communications échangées par les individus dans la sphère numérique.

## LES PRINCIPES DE LA DÉTECTION POSÉS PAR L'ARTICLE L. 851-3 DU CODE DE LA SÉCURITÉ INTÉRIEURE

*« I.- (..) pour les seules finalités prévues aux 1°, 2° et 4° de l'article L. 811-3, à la demande des services spécialisés de renseignement mentionnés à l'article L. 811-2, peuvent être autorisés, sur les données transitant par les réseaux des opérateurs et des personnes mentionnées à l'article L. 851-1, des traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler des ingérences étrangères, des menaces pour la défense nationale ou des menaces terroristes.*

*Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1 ainsi que les adresses complètes de ressources utilisées sur internet, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations, documents ou adresses se rapportent. / (…)*

*Dans le respect du principe de proportionnalité, l'autorisation du Premier ministre précise le champ technique de la mise en œuvre de ces traitements.*

*II.- La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. (…)*

*IV.- Lorsque les traitements (…) détectent des données susceptibles de caractériser l'existence d'une menace, le Premier ministre (…) peut autoriser, après avis de la Commission nationale de contrôle des techniques de renseignement (..), l'identification de la ou des personnes concernées et le recueil des données y afférentes. (…) ».*

### 2.1.2. | Un encadrement juridique et technique très étroit

Si l'algorithme a été conçu comme un outil de détection avancée des menaces, son intégration dans le droit commun du renseignement a suscité d'importantes craintes en raison des potentialités des traitements automatisés sur lesquels la technique repose. L'usage de ces systèmes comporte en effet des risques intrinsèques d'atteinte aux droits et libertés, en particulier au droit au respect de la vie privée et des données personnelles, du seul fait qu'ils permettent le traitement et l'analyse massifs de données numériques.

Ces craintes, qui trouvent un écho renouvelé dans les préoccupations majeures soulevées par le débat public sur la capacité à expliquer les résultats de l'intelligence artificielle et l'IA de confiance, justifient que l'emploi de l'algorithme ait fait l'objet d'un encadrement juridique particulièrement étroit, qui, hormis l'élargissement de son champ d'emploi (voir ci-dessus), s'est plutôt renforcé au fil du temps.

**Il faut ainsi tout d'abord relever que le recours aux traitements automatisés fait l'objet d'un régime d'autorisation plus strict que celui appliqué aux autres techniques de renseignement, en vertu des dispositions de l'article L. 851-3 du code de la sécurité intérieure :**

- l'algorithme ne peut être autorisé qu'en vue de détecter des connexions susceptibles de révéler des ingérences étrangères, des menaces pour la défense nationale ou des menaces terroristes. À ce jour, il ne peut donc être fondé que sur **trois finalités**[36] seulement parmi les huit prévues par les articles L. 811-3 et L. 855-1 du code de la sécurité intérieure ;

36. La proposition de loi visant à sortir la France du piège du narcotrafic, adoptée par le Parlement les 28 et 29 avril 2025, prévoit en effet une extension de la technique à la finalité mentionnée au 6° de l'article L. 811-3 du CSI. Ses dispositions font toutefois l'objet de trois saisines du Conseil constitutionnel du 12 mai 2025 (saisines 2025-885 DC). À la date de finalisation du présent rapport, la décision du Conseil constitutionnel n'est pas encore intervenue.

- seuls les six services spécialisés de renseignement, dits **services du premier cercle**, sont autorisés à y avoir recours ;

- le fonctionnement en deux temps de la technique nécessite l'obtention par les services de **deux autorisations successives** du Premier ministre, prises chacune après avis de la CNCTR, portant sur la mise en œuvre d'un traitement automatisé puis sur la levée de l'anonymat en cas de détection d'une menace ;

- l'autorisation initiale de mise en œuvre d'un traitement automatisé est limitée à **deux mois**, et, si elle est renouvelable pour quatre mois dans les conditions de droit commun, la demande de renouvellement doit faire l'objet d'une **motivation particulière** comportant, outre les éléments prévus à l'article L. 821-2 du CSI[37], un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements ;

- enfin, **l'urgence** permettant au Premier ministre d'ordonner la mise en œuvre immédiate d'une technique en cas d'avis défavorable de la CNCTR, prévue à l'article L. 821-1 du code de la sécurité intérieure, ne peut être invoquée pour la mise en place ou le renouvellement d'un algorithme.

**En outre, des garanties renforcées ont été prévues initialement ou ajoutées afin de limiter le caractère attentatoire de la technique :**

- s'agissant des **données traitées**, si les traitements automatisés ont été étendus aux URL en 2021, cet élargissement du champ d'investigation de la technique s'est accompagné d'un aménagement du régime de toutes les

37. L'article L. 821-2 du CSI prévoit que les demandes de techniques de renseignement doivent préciser : « *1° La ou les techniques à mettre en œuvre ; 2° Le service pour lequel elle est présentée ; 3° La ou les finalités poursuivies ; 4° Le ou les motifs des mesures ; 5° La durée de validité de l'autorisation ; 6° La ou les personnes, le ou les lieux ou véhicules concernés .*

*Pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules peuvent être désignés par référence aux personnes faisant l'objet de la demande.*

*Lorsqu'elle a pour objet le renouvellement d'une autorisation, la demande expose les raisons pour lesquelles ce renouvellement est justifié au regard de la ou des finalités poursuivies* ».

données visées par l'algorithme en vue de circonscrire au mieux les atteintes portées aux libertés. Les données détectées comme étant susceptibles de caractériser l'existence d'une menace dans le cadre d'une alerte ne peuvent être conservées que pendant soixante jours, sans possibilité de prolongation de ce délai d'exploitation jusqu'à quatre années comme prévu pendant la phase d'expérimentation. En outre, la loi impose désormais que les données non détectées par les traitements comme susceptibles de révéler une menace doivent, elles, être immédiatement détruites.

- de plus, parce que le caractère potentiellement très attentatoire des traitements automatisés nécessite d'opérer **un examen exigeant de la proportionnalité** entre les atteintes portées à la protection de la vie privée et des données personnelles et la protection des intérêts fondamentaux de la Nation, des mécanismes particuliers de **contrôle de l'algorithme** sont prévus. En plus des évaluations et contrôles parlementaires imposés dans le cadre des expérimentations susmentionnées, le code de la sécurité intérieure prend soin de conférer à la CNCTR les prérogatives nécessaires au bon exercice de son contrôle de la technique, novatrice et complexe. En vertu du II de l'article L. 851-3 de ce code, **la commission doit ainsi disposer** « ***d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies*** », et elle doit être « ***informée de toute modification apportée aux traitements et paramètres*** ». S'y ajoute aussi la faculté pour la commission d'émettre des recommandations sur la technique de l'algorithme, en sus de la possibilité générale qu'elle tient de l'article L. 833-6 du même code.

**Enfin, l'encadrement de l'algorithme porte aussi sur le dispositif technique permettant sa mise en œuvre, remanié pour être plus protecteur.**

La pérennisation de la technique s'est accompagnée de la consécration au niveau législatif de l'architecture technique et organisationnelle mise en place en 2017 pour confier l'exécution centralisée des algorithmes au GIC.

**L'architecture technique de mise en œuvre des algorithmes résulte des travaux concertés des services du Premier ministre, du GIC, et de la CNCTR** lors de la construction du dispositif d'exécution du premier algorithme en 2016-2017, qui ont cherché un point d'équilibre entre l'efficacité de la technique et la limitation au strict nécessaire des atteintes portées au respect de la vie privée et au secret des correspondances.

Lors de l'examen du projet de la loi sur le renseignement en 2015, un mécanisme consistant à demander aux opérateurs de mettre en œuvre eux-mêmes les traitements automatisés en plaçant des dispositifs de détection en plusieurs points de leurs réseaux avait été envisagé. Cette modalité d'exécution a toutefois été abandonnée au vu de ses inconvénients pratiques (risque de perturbation de la sécurité de ces réseaux, amoindrissement de la capacité de détection du fait de la multiplicité des réseaux, divulgation aux opérateurs des paramètres de détection retenus[38]). Conséquemment, le gouvernement s'est orienté vers une modalité d'exécution centralisée des algorithmes, consistant à dupliquer les flux de données de connexion sur les réseaux des opérateurs puis à les acheminer vers le GIC, chargé d'exécuter tous les traitements automatisés prévus par l'article L. 851-3 du code de la sécurité intérieure.

Consultée sur un premier projet d'architecture générale reprenant ce principe, la CNCTR a formulé, dans une délibération classifiée, plusieurs recommandations, dont celle préconisant que le dispositif

38. Voir étude d'impact relative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, 11 mai 2021 : https://www.assemblee-nationale.fr/dyn/15/textes/l15b4104_etude-impact.pdf.

centralisé soit placé sous la seule et entière responsabilité du GIC. Faisant écran entre les données analysées par les algorithmes et les services de renseignement ayant demandé leur mise en œuvre, cette centralisation au GIC est apparue comme un garde-fou technique essentiel pour s'assurer que les services de renseignement ne puissent à aucun moment accéder directement aux données soumises aux traitements automatisés. Corrélativement, la commission a préconisé la mise en place d'un dispositif de traçabilité de tous les accès au dispositif, aux fins de contrôler son étanchéité vis-à-vis des services de renseignement et, plus largement, de tout agent hormis ceux individuellement habilités à intervenir dans l'exécution des traitements automatisés. Enfin, la CNCTR a recommandé la fixation d'une durée de stockage des données soumises aux traitements automatisés au sein du GIC très brève, limitée au temps strictement nécessaire pour permettre l'exécution des algorithmes

Reprenant l'ensemble de ces observations et recommandations, le Premier ministre a fixé les règles générales de mise en œuvre des algorithmes dans une décision classifiée du 27 avril 2017. Le VI de l'article L. 851-3 du code de la sécurité intérieure en reprend le principe, en vertu duquel un service du Premier ministre, distinct des services de renseignement, est seul habilité à exécuter les traitements et opérations mis en œuvre dans le cadre de la surveillance algorithmique.

## DES CONDITIONS DE MISE EN ŒUVRE AUJOURD'HUI CONFORMES AUX EXIGENCES EUROPÉENNES

**L'application de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et la jurisprudence de la Cour européenne des droits de l'homme (CEDH) :**

Appliquant à la surveillance électronique le principe du droit au respect de la vie privée et familiale, du domicile et de la correspondance, protégé par l'article 8 de la Convention, la CEDH s'est prononcée sur la conventionalité de dispositifs de surveillance de masse, à laquelle peut se rattacher la technique de l'algorithme pour les besoins de l'analyse juridique. Dans ses deux arrêts de sa grande chambre rendu le 25 mai 2021, elle a notamment considéré que les États parties à la Convention pouvaient, pour préserver leur sécurité, recourir à la surveillance de masse des communications électroniques, qu'il s'agisse du contenu de celles-ci ou des métadonnées rattachées, à la condition que le dispositif de surveillance en cause soit précisément déterminé par la loi, qu'il soit nécessaire et qu'il présente des garanties procédurales « de bout en bout » (CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, req. nos 58170/13, 62322/14 et 24960/15 CEDH, 25 mai 2021, *Centrum för Rättvisa c. Suède*, req. n° 35252/08)[39].

L'encadrement juridique étroit entourant aujourd'hui la mise en œuvre de la technique de l'algorithme doit permettre de regarder ce dispositif de détection comme répondant aux exigences posées par la CEDH.

**La question de l'application du droit de l'Union européenne.**

Si, comme indiqué en introduction, les techniques de renseignement ne sont en principe pas régies par les réglementations européennes, ces dernières peuvent néanmoins avoir une incidence sur leurs

39. Pour une présentation détaillée de ces décisions et des exigences posées par la CEDH, voir le 6ème rapport d'activité 2021 de la CNCTR, partie 1.2 p. 48.

conditions de mise en œuvre. Ainsi, dans une très remarquée série de décisions rendues en octobre 2020, la CJUE a jugé que le droit européen régissant le secteur des communications électroniques et données numériques s'opposait à des mesures législatives imposant, à titre préventif, une conservation généralisée et indifférenciée des données de connexion (CJUE, 6 octobre 2020, *La Quadrature du Net et autres*, aff. C-511/18, C-512/18, C-520/18 et C-623/17). Or, la mise à disposition de ces données est nécessaire pour mettre en œuvre certaines techniques de renseignement.

Cette appréhension du droit du renseignement par le droit de l'Union aurait pu se traduire par une censure des dispositions nationales au motif de leur incompatibilité avec les dispositions européennes régissant les activités numériques. Toutefois, par une série de décisions du 21 avril 2021, le Conseil d'Etat a validé le principe de l'obligation faite aux opérateurs de communications électroniques et aux fournisseurs d'accès à internet de conserver de manière généralisée et indifférenciée les données de connexion, sous réserve du constat régulier de la persistance d'une menace suffisante pour la sécurité nationale (CE, Assemblée, 21 avril 2021, *French Data Network et autres*, n° 393099 ; *La Quadrature du Net et autres*, n° 394922 n°397851 ; *Association Igwan.net*, n° 397844 ; *Société Free Mobile*, n° 424717 et *Société Free* n° 424718). Par ailleurs, les réserves émises ou incompatibilités relevées dans ces décisions concernant le régime de conservation des données et l'obligation de contrôle préalable des techniques par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, ont été levées par l'adoption de la loi PATR du 30 juillet 2021[40].

40. Voir sur ces points, 6ème rapport d'activité 2021 de la CNCTR : annexe n° 4, délibération de la CNCTR n° 4/2021 du 30 avril 2021 et annexe n° 5, décision du Conseil d'État statuant au contentieux.

## 2.2. Un contrôle rigoureux du déploiement des algorithmes

### 2.2.1. Un contrôle *a priori* très poussé

Le contrôle *a priori* de la CNCTR sur les algorithmes se doit d'être particulièrement rigoureux. Il s'avère significativement plus exigeant que pour les autres techniques de renseignement, en particulier pour ce qui est de l'appréciation de la légalité et de la proportionnalité des demandes d'autorisation initiales d'un nouvel algorithme. Par ailleurs, la commission statue toujours sous la forme d'une délibération classifiée prise par le collège dans sa formation plénière, permettant de développer un avis aussi détaillé que nécessaire et d'introduire les éventuelles restrictions qui lui semblent s'imposer.

Ce contrôle nécessite l'engagement, par le service demandeur et le GIC, d'études et de travaux préparatoires lourds, nécessaires pour que la commission soit en position d'apprécier la pertinence des paramètres envisagés pour l'algorithme et le degré d'intrusivité des traitements correspondants, en plus de l'examen de la justification au fond du recours à la technique et du respect par la demande de la légalité externe. Le paramétrage de l'algorithme conditionne l'efficacité opérationnelle du dispositif de détection aussi bien qu'il constitue la garantie d'un traitement, certes non individualisé, mais circonscrit et proportionné dans ses effets.

Pour veiller à l'équilibre entre ces deux impératifs, le contrôle réalisé par la CNCTR s'appuie sur un audit du paramétrage et des principes de fonctionnement du dispositif algorithmique proposé, le cas échéant accompagné d'une vérification de son code source. Son examen porte alors sur tous les éléments retenus par le

service demandeur pour concevoir son algorithme, en particulier les comportements recherchés, ainsi que sur les modélisations établies en vue de vérifier la conformité du traitement à sa description et à la motivation exposées par le service et évaluer son caractère suffisamment discriminant. La commission veille particulièrement à ne pas se trouver face à une « boîte noire ».

Les examens et vérifications approfondies ainsi réalisés, conjugués au dialogue noué au cours des phases d'élaboration et de modification de chaque algorithme avec le GIC et le service demandeur, permettent un développement concerté de cette technique, propre à garantir son acceptabilité. Les cinq algorithmes actuellement mis en œuvre ont tous été élaborés à l'issue d'une telle démarche associant étroitement la CNCTR, le GIC et les services demandeurs à l'élaboration du dispositif[41].

Si le contrôle réalisé sur les demandes de renouvellement devient progressivement moins sensible dès lors que le fonctionnement de l'algorithme s'avère stable, il est néanmoins assuré avec une vigilance renforcée afin de garantir le respect du cadre légal et la proportionnalité de la technique. Il tient également compte de l'exposé de ses résultats opérationnels par le GIC et le service concerné. Par ailleurs, signe de l'importance accordée par la CNCTR au contrôle des demandes de renouvellement des algorithmes, leur examen est toujours effectué par son collège siégeant en formation plénière, bien que la loi ne l'impose pas.

Le contrôle exigeant réalisé par la CNCTR peut être illustré par le processus suivi lors de la mise en place du premier algorithme en 2017[42].

Après des échanges nourris sur l'architecture à retenir pour les algorithmes, la CNCTR a été saisie d'une demande tendant à la

41. Voir p. 42 du présent rapport.

42. Ce processus est détaillé dans le 2ème rapport d'activité 2017 de la CNCTR, disponible sur son site internet.

première mise en œuvre d'un traitement automatisé sur le fondement de l'article L. 851-3 du code de la sécurité intérieure. Elle a procédé à un audit préalable sur pièces et sur place, afin de vérifier que l'algorithme, notamment son code source, était conforme à la description faite dans la demande. Par une délibération classifiée adoptée en formation plénière le 26 juillet 2017, elle a constaté que le traitement présenté correspondait, par ses caractéristiques techniques et sa fonction, à la définition légale de l'algorithme et a acté sa conformité à la description du service. Elle a aussi considéré que le recours à ce traitement ne porterait pas à la vie privée une atteinte disproportionnée à la menace terroriste à prévenir. Néanmoins, elle a émis un avis défavorable à la mise en œuvre du traitement, après avoir relevé que sa mise en œuvre n'était pas entourée de suffisamment de garanties.

Saisie d'une nouvelle demande portant sur le même algorithme, la CNCTR, après avoir pris acte des nouvelles garanties proposées, a émis le 5 octobre 2017 un avis favorable à une première mise en œuvre de ce traitement pour deux mois, conformément au II de l'article L. 851-3 du code de la sécurité intérieure. Saisie d'une demande de renouvellement à l'issue de ce délai, la commission a formulé un avis favorable à ce renouvellement, sous réserve toutefois qu'il soit à nouveau limité à une durée de deux mois. Au vu des premiers résultats, un réexamen à brève échéance du traitement automatisé a été estimé nécessaire pour s'assurer de la pertinence et de la fiabilité de ses caractéristiques techniques. Cet avis a été suivi par le Premier ministre.

Quant au contrôle réalisé sur les demandes de levée de l'anonymat, il s'avère d'autant plus simple et aisé que le paramétrage du dispositif algorithmique a été réalisé et vérifié de manière appropriée. Il a permis à la commission de détecter toute instabilité des traitements, qui se traduirait par exemple par une production d'alertes anormale au regard des travaux de mise au

point, et de recommander leur interruption immédiate. Attestant du travail réalisé sur ce point, l'étude d'impact du 11 mai 2021 précitée[43] relevait par exemple que le paramétrage des trois algorithmes en fonctionnement en 2020 avait permis de contenir la fréquence des alertes tout en maintenant un seuil de détection utile.

### 2.2.2.| Un contrôle *a posteriori* diversifié

Le contrôle *a posteriori* le plus usuel tient à l'appréciation par la CNCTR des résultats des algorithmes exposés par les services lors de leurs demandes de renouvellement ou de modification, occurrences pour lesquelles la loi a pris de soin de donner à la CNCTR les moyens d'un contrôle efficace en prévoyant en particulier qu'elle doit être « *informée de toute modification apportée aux traitements et paramètres* » des traitements automatisés et disposer « *d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies* »[44].

À ces contrôles réguliers s'ajoute, plus ponctuellement, l'examen des bilans généraux que peut établir le Premier ministre sur la surveillance algorithmique, objets de rapports d'évaluation classifiés permettant à ses destinataires, CNCTR et DPR, d'apprécier l'utilité même de la technique et la maîtrise de son caractère attentatoire à la protection de la vie privée et des données personnelles, ou de rapports publics à destination, en particulier, de la représentation nationale.

À côté de ces contrôles sur pièces, des contrôles sont également opérés, par exemple consécutivement à des évolutions techniques ou organisationnelles, au travers en particulier de travaux d'audit des codes des algorithmes, de contrôle des modalités pratiques de

43. Voir note 38.

44. Article L. 851-3 du CSI.

la centralisation au GIC, et d'examen des informations et données recueillies par le truchement de traitements automatisés. À cet égard, la commission s'assure du respect, non seulement des exigences légales, mais aussi des recommandations formulées dans le cadre de l'élaboration de l'architecture technique des algorithmes.

L'usage de l'algorithme par la politique publique au renseignement en France ne fait pas de cette technique une surveillance de masse, puisqu'il ne permet pas aux services de renseignement de connaître les occupations d'une multitude de personnes précisément identifiées ou identifiables. A l'inverse, il a pour finalité de mettre en évidence, de façon anonyme, des indices, à partir desquels une levée d'anonymat est possible, sous un strict contrôle.

La loi a permis cet usage pour améliorer la capacité des services de renseignement à détecter des menaces graves ; elle a assuré l'indispensable équilibre du système en donnant à la CNCTR une faculté de contrôle de bout en bout. La commission exerce pleinement cette faculté.

Il appartient au législateur d'apprécier si l'intérêt général justifie l'emploi de la technique de l'algorithme à l'une des finalités limitativement déterminées par le code de la sécurité intérieure. D'abord réservé à la lutte contre le terrorisme, cet emploi a été étendu à la lutte contre les ingérences étrangères et il le sera demain à la lutte contre le narcotrafic, dont il apparaît qu'il est devenu une menace pour le fonctionnement normal de nos institutions, ainsi que le relevait la commission dans son rapport d'activité 2023.

Pour sa part, la CNCTR continuera, en lien avec les services de renseignement et le Groupement interministériel de contrôle, à veiller par son contrôle à l'équilibre dont elle est la garante.

# Annexes

# 1. Évolution de la composition du collège au cours de l'année 2024

La composition du collège de la CNCTR a été sensiblement modifiée au cours de l'année 2024.

En effet, le 2 octobre 2024, les mandats de Mme Françoise Sichler-Ghestin, conseillère d'État honoraire, et de M. Gérard Poirotte, conseiller honoraire à la Cour de cassation, se sont achevés. Ils ont été remplacés par Mme Magali Ingall-Montagnier, conseillère à la Cour de cassation et M. Didier Chauvaux, conseiller d'État honoraire. Par ailleurs, la dissolution de l'Assemblée nationale intervenue le 9 juin 2024 a conduit à mettre un terme aux mandats de Mme Michèle Tabarot et de M. Yannick Chenevard. Ils ont été remplacés par Mme Émilie Bonnivard, députée de la Savoie, et M. Christophe Naegelen, député des Vosges, désignés le 6 novembre 2024.

À la fin de l'année 2024, le collège de la CNCTR était composé des **neuf membres** suivants :

- **M. Serge Lasvignes**, conseiller d'État honoraire, président ;
- **Mme Chantal Deseyne**, sénatrice d'Eure-et-Loir ;
- **M. Jérôme Darras**, sénateur du Pas-de-Calais ;
- **Mme Émilie Bonnivard**, députée de la Savoie ;
- **M. Christophe Naegelen**, député des Vosges ;
- **M. Didier Chauvaux**, conseiller d'État honoraire ;
- **Mme Solange Moracchini**, avocate générale honoraire à la Cour de cassation ;
- **Mme Magali Ingall-Montagnier**, conseillère à la Cour de cassation ;
- **M. Philippe Distler**, personnalité qualifiée en matière de communications électroniques.

**Suite à la démission du président Lasvignes en janvier 2025, Mme Solange Moracchini a été nommée présidente par intérim[1], puis, par décret du 28 mars 2025[2], M. Vincent Mazauric a été nommé président de la commission.**

1. Voir décret du 31 janvier 2025 du Président de la République, nommant Mme Moracchini, membre du collège, présidente par intérim à compter du 1er février 2025.
2. Voir le décret du 28 mars 2025 du Président de la République portant nomination du président de la Commission nationale de contrôle des techniques de renseignement, publié au Journal officiel le 29 mars.

Les modalités de désignation ou de nomination des membres sont fixées par l'article L. 831-1 du code de la sécurité intérieure et, le cas échéant, par les dispositions de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes. À l'exception des membres parlementaires, leur mandat est de six ans et n'est pas renouvelable. Les membres du Conseil d'État et de la Cour de cassation sont renouvelés par moitié tous les trois ans. Par ailleurs, à l'exception de la personnalité qualifiée, la loi prévoit que les modalités de désignation ou de nomination des membres de la commission assurent l'égale représentation des hommes et des femmes.

En vertu de l'article 5 de la loi du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes, un membre nommé en remplacement d'un membre ayant cessé son mandat avant son terme normal est désigné pour la durée du mandat restant à courir. Si cette durée est inférieure à deux ans, ce mandat n'est pas pris en compte pour l'application de la règle de non-renouvellement fixée à l'article L. 831-1 du CSI.

# 2. Les moyens de la CNCTR en 2024

## 2.1. Les ressources humaines

Depuis fin novembre 2023, quatre des neuf membres du collège de la commission exercent leur mandat à temps plein. Il s'agit du président de la CNCTR, des deux membres de la Cour de cassation et de la personnalité qualifiée.

Les dispositions du code de la sécurité intérieure imposent un délai de vingt-quatre heures à la CNCTR pour rendre ses avis sur les demandes de mise en œuvre de techniques de renseignement dont l'examen en formation collégiale n'est pas requis. Ces avis ne peuvent être rendus que par les membres ayant la qualité de magistrat. Lorsque la demande relève de la formation collégiale plénière ou de la formation collégiale restreinte, ou qu'elle est renvoyée devant une telle formation, le délai est porté à soixante-douze heures. En conséquence, ces formations collégiales se réunissent sauf exception trois fois par semaine, les lundis, mercredis et vendredis. Chaque mois, la CNCTR tient une réunion solennelle de l'ensemble de ses membres en une formation plénière. Ces réunions examinent les projets de délibérations les plus importantes et comportent un temps consacré à l'activité de la commission, qu'il s'agisse de sujets de fond comme d'éléments statistiques.

En parallèle de ces formations collégiales, de fréquentes réunions, présentations et auditions sont organisées avec les services de renseignement dans les locaux de la commission afin d'éclairer le collège sur des sujets d'ordre technique ou juridique.

Les membres exerçant leur mandat à temps plein participent également aux contrôles menés dans les services.

En fin d'année 2024, la CNCTR exerçait sa mission grâce à une équipe de 22 agents, dirigée par une secrétaire générale et composée d'une conseillère placée auprès du président, de 14 chargés de mission et de 4 agents affectés aux fonctions de soutien : une responsable des questions budgétaires et de ressources humaines chargée d'encadrer le pôle du secrétariat, deux assistantes de direction et un agent polyvalent chargé en outre des fonctions d'officier de sécurité adjoint. La CNCTR a par ailleurs renforcé son pôle des systèmes d'information grâce au recrutement d'un administrateur réseaux.

Les chargés de mission de la CNCTR sont des agents de catégorie A+ ou assimilés, dont le rôle principal est d'instruire les demandes de mise en œuvre des techniques de renseignement et de conduire les contrôles *a posteriori*, sous la supervision d'un membre de la commission.

Ils sont soit des agents publics détachés ou mis à disposition : magistrats judiciaires et administratifs, commissaire de police, officier de gendarmerie, ingénieur en chef de l'armement, inspecteur des douanes, soit des agents contractuels, ingénieurs notamment.

Le personnel du secrétariat est, quant à lui, composé de deux fonctionnaires titulaires et de deux agents contractuels.

L'équipe est paritaire : 11 hommes et 11 femmes. La moyenne d'âge des agents est de 39 ans.

Conformément aux dispositions de l'article L. 832-5 du code de la sécurité intérieure, l'ensemble du personnel de la Commission est habilité au secret de la défense nationale.

## 2.2. Le budget

Les crédits alloués par le Parlement à la CNCTR en loi de finances le sont dans le cadre de la mission « Direction de l'action du gouvernement » qui regroupe les crédits et les emplois des services du Premier ministre et des autorités indépendantes. Deux programmes composent cette mission : le programme 129 « Coordination du travail gouvernemental » et le programme 308 « Protection des droits et libertés ». Le programme 308 regroupe les crédits de dix autorités indépendantes exerçant leurs missions

dans le champ de la protection des droits de l'homme et des libertés publiques et individuelles, dont la CNCTR[3].

La loi de finances pour 2024[4] a attribué à la CNCTR des crédits d'un peu plus de 3 millions d'euros pour ses dépenses de personnel (titre II) et d'un peu plus de 480 000 euros pour ses dépenses de fonctionnement, représentant environ 2,5 % du budget du programme 308. Les crédits de fonctionnement initialement prévus ont toutefois été sensiblement affectés par les annulations de crédits intervenues en début d'année 2024[5] et réduits à un peu moins de 450 000 euros (soit une réduction de plus de 7 %).

Si les crédits alloués en 2024 ont, en particulier, permis de constituer un pôle des systèmes d'information composé d'agents dédiés, avec notamment l'objectif de sécuriser le système d'information interne de la commission, l'augmentation constante de son volume d'activité et le renforcement de ses missions au gré des modifications législatives et réglementaires intervenues dans le domaine du renseignement placent ses effectifs et ses moyens sous tension.

Alors que dans le cadre de la loi de finances pour 2025[6], aucune création de poste n'a été prévue et que ses crédits de fonctionnement ont de nouveau été diminués, **la CNCTR souligne la tension croissante entre l'évolution des modalités d'exercice de ses missions** (hausse du nombre de demandes, augmentation du volume de données recueillies, complexité accrue du contrôle…) **et les moyens dont elle dispose**. Cette tension concerne également les fonctions de management et de support dont les

3. Outre la CNCTR, le programme 308 regroupe ainsi les crédits alloués au Défenseur des droits, à la Commission nationale de l'informatique et des libertés (CNIL), au Contrôleur général des lieux de privation de liberté (CGLPL), à la Commission d'accès aux documents administratifs (CADA), à la Commission du secret de la défense nationale (CSDN), à la Haute autorité pour la transparence de la vie publique (HATVP), à l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), au Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE) et à la Commission nationale consultative des droits de l'homme (CNCDH).

4. Voir loi n° 2023-1322 du 29 décembre 2023 de finances pour 2024.

5. Voir le décret n° 2024-124 du 21 février 2024 portant annulation de crédits.

6. Voir loi n° 2025-127 du 14 février 2025 de finances pour 2025.

effectifs ne permettent pas, en l'état, de sécuriser de façon entièrement satisfaisante le fonctionnement de la commission.

# 3. Les relations extérieures

Au cours de l'année 2024, la commission a poursuivi son dialogue constructif avec ses partenaires institutionnels, le monde universitaire mais également ses homologues étrangers. Pour la première fois depuis sa création, elle a organisé deux colloques ouverts au public permettant ainsi un accès plus large à ses missions et à ses analyses (3.1). Par ailleurs, comme les précédentes années, la commission est intervenue à plusieurs reprises devant le Parlement (3.2) et a dispensé des formations au bénéfice de diverses entités publiques (3.3). Ces nombreux échanges et interactions, tant au niveau national (3.4) qu'international (3.5), permettent à la commission d'exposer son point de vue sur le cadre légal du renseignement. Ils favorisent la diffusion de la connaissance de ce cadre légal, une amélioration des pratiques et un enrichissement mutuel.

## 3.1. Une ouverture des missions et analyses de la commission au grand public à travers l'organisation de deux colloques

**Une conférence internationale co-organisée avec la revue Etudes françaises de renseignement et du cyber (EFRC)**

Le **15 octobre 2024**, la CNCTR, a co-organisé avec la revue Etudes françaises de renseignement et du cyber (PUF), **une conférence consacrée aux enjeux du contrôle des services de renseignement et plus particulièrement au dialogue entre les contrôleurs.**

Organisée autour de trois tables rondes thématiques, elle a réuni des responsables publics du monde du renseignement, des magistrats, des membres d'instances de contrôle d'autres Etats européens, des universitaires ou encore des experts en techniques de surveillance. Les échanges ont permis de débattre des modalités de contrôle des données et des technologies, d'examiner différents modèles de contrôle des services de renseignement mis en œuvre en Europe ou encore de s'interroger sur la co-existence, en France, de multiples contrôleurs des services de renseignement qu'il s'agisse du Parlement, du Conseil d'Etat, de la Cour des comptes, d'autorités administratives indépendantes ou d'entités d'inspection ou de contrôle interne.

Pour la première fois depuis la création de la commission, cette manifestation a été ouverte au grand public. Elle a réuni près de 350 participants[7].

**Un colloque co-organisé avec la Commission nationale de l'informatique et des libertés (CNIL) - « La surveillance dans tous ses états. Quelle éthique pour protéger nos libertés ? ».**

Depuis plusieurs années, la CNIL organise des débats publics autour des nouveaux enjeux du numérique, au croisement d'expertises de terrain et scientifiques : c'est l'objectif des évènements « air »[8]. En 2024, la CNCTR a été invitée par la CNIL à co-organiser cet évènement autour de la thématique de **la surveillance sous toutes ses formes et ses enjeux éthiques**.

Afin de proposer une réflexion prospective sur la surveillance, ce colloque, qui s'est tenu le **19 novembre 2024**, a rassemblé des responsables publics du monde du renseignement, des chercheurs en sciences politiques, des sociologues, des experts en

7. Voir les actes du colloque publiés dans le numéro n°4 de la revue EFRC ou sur le site internet Cairn https://shs.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2024-2?lang=fr

8. Pour « avenirs, innovations, révolutions ».

techniques de surveillance, des institutionnels et des associations de protection des libertés individuelles, qui ont pu échanger lors de deux tables rondes consacrées aux enjeux de la surveillance par les pairs et interpersonnels et à l'éthique des services de renseignements[9].

De format hybride (visioconférence et présentiel), cette manifestation a réuni près de 1 700 personnes autour de ces thématiques, permettant ainsi une ouverture plus grande aux enjeux de la surveillance, et en particulier à celle menée par les services de renseignement, au bénéfice de tous les citoyens.

La CNCTR a aussi poursuivi son effort de mise à disposition du grand public d'informations, aussi détaillées que le permettent les exigences de protection du secret de la défense nationale, sur sa mission et l'exercice de son action de contrôle.

Dans le prolongement de la refonte de son site Internet[10] intervenu au cours de l'année 2023, la commission a enrichi les ressources qui y sont accessibles : rapports d'activités, fiches thématiques, traductions en anglais.

## 3.2. Un dialogue entretenu avec le Parlement

Au cours de l'année 2024, le président de la CNCTR a été auditionné à plusieurs reprises par le Parlement. Au-delà de la possibilité ouverte par l'article L. 833-11 du CSI au président de l'Assemblée nationale, au président du Sénat et à la délégation parlementaire au renseignement de saisir pour avis la commission, ces sollicitations manifestent le dialogue entretenu d'année en année avec le Parlement.

9. La CNIL et la CNCTR ont publié en mars 2025 reprenant les différentes thématiques abordées lors de l'événement sous la forme d'entretiens et de témoignages. Voir les sites internet de la CNCTR ou de la CNIL : https://www.cnctr.fr/actes-colloque-air2024#le-cahier-air2024 et https://www.cnil.fr/fr/cahier-air2024.

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

Le président Lasvignes a été entendu à deux reprises par le Sénat. En avril, à l'initiative de Mme Agnès Canayer, rapporteure de la **proposition de la loi visant à prévenir les ingérences étrangères en France**[11] pour la commission des lois, il a notamment été interrogé sur l'extension de la technique dite de l'algorithme aux finalités mentionnées aux 1° et aux 2° de l'article L. 811-3 du CSI (voir l'étude consacrée à cette technique, p. 141). En juin, il a présenté aux commissions des lois et de la défense le rapport d'activité de la CNCTR pour l'année 2023.

Il a été auditionné à deux reprises par l'Assemblée nationale. En mars 2024, M. Sacha Houlié, président de la commission des lois, auteur et rapporteur de la **proposition de la loi visant à prévenir les ingérences étrangères en France**[12], l'a invité à s'exprimer sur l'opportunité et les enjeux juridiques d'une extension de la technique de l'algorithme à de nouvelles finalités. En septembre, il a pu échanger avec Mme Yaël Braun-Pivet, présidente de l'Assemblée nationale, afin de lui présenter le rapport d'activité de la CNCTR pour l'année 2023 et les sujets de vigilance mis en avant par la commission dans le cadre de celui-ci.

Par ailleurs, la délégation parlementaire au renseignement, qui comprend à la fois des élus de l'Assemblée nationale et du Sénat, l'a également entendu à deux reprises en 2024. En mai, il a été auditionné notamment sur le bilan d'activité de la CNCTR pour l'année 2023, sur l'extension de la technique de l'algorithme dans le cadre de la proposition de loi visant à prévenir les ingérences étrangères en France ainsi que sur les perspectives et enjeux identifiés par la commission pour les prochaines années. En novembre, il a pu échanger avec la délégation sur l'activité des services de renseignement dans le contexte de l'organisation des Jeux olympiques et paralympiques ainsi que sur les évolutions possibles du cadre légal.

11. Voir le dossier législatif sur le site du Sénat : Ingérences étrangères en France - Sénat.
12. Voir le dossier législatif sur le site de l'Assemblée nationale : Prévenir les ingérences étrangères en France - Dossiers législatifs - 16e → 16e législature - Assemblée nationale.

## 3.3. Les formations auxquelles la commission a contribué

En 2024, la commission a de nouveau contribué à l'effort de formation des agents des services de renseignement ainsi que des cadres de leurs ministères de tutelle pour développer en leur sein la connaissance du cadre juridique applicable aux techniques de renseignement. La commission est ainsi intervenue à près d'une dizaine de reprises en 2024 devant les auditeurs de l'**Académie du renseignement**.

Par ailleurs, elle a contribué à trois sessions de formations continues dispensées par l'**École nationale de la magistrature**.

## 3.4. Les autres interlocuteurs institutionnels de la commission

Le président Lasvignes a été entendu à deux reprises par le Conseil d'État : une première fois, en janvier 2024, dans le cadre des travaux destinés à son étude annuelle consacrée à la souveraineté[13], une seconde fois, afin de présenter le rapport d'activité de la commission pour l'année 2023 à la section de l'intérieur.

## 3.5. Les relations internationales de la commission

Au cours de l'année 2024, la CNCTR a entretenu le dialogue avec ses homologues étrangers dans le cadre de réunions bilatérales mais également multilatérales.

13. Voir : https://conseil-etat.fr/publications-colloques/etudes/etude-annuelle-sur-la-souverainete.

Une délégation de la commission a ainsi participé le 13 juin 2024, à Venise, à la **Conférence internationale sur la protection de la vie privée**, qui réunit chaque année des autorités nationales de contrôle de nombreux pays et des universitaires.

Les échanges ont notamment porté sur les différentes modalités de traitement, en France et dans d'autres pays tels que les États-Unis ou encore le Canada, des réclamations ou recours des personnes souhaitant vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à leur égard.

Par ailleurs, lors du colloque organisé le 15 octobre 2024[14], une table ronde a été consacrée à un échange entre des représentants des organes de contrôle des services de renseignement de l'Allemagne[15], du Danemark[16] et du Royaume-Uni[17].

14. Voir ci-dessus.
15. *G 10 - Kommission.*
16. *Danish Intelligence Oversight board (TET).*
17. *Investigatory Powers Commissionner's Office (IPCO).*

# 4. Glossaire

## A

- **Algorithme**

  Traitement automatisé de données de connexion dont la mise en œuvre, prévue à l'article L. 851-3 du code de la sécurité intérieure, ne peut être autorisée que pour les seuls besoins de la prévention du terrorisme.

  L'algorithme vise à déceler, parmi des données de connexion transitant sur les réseaux des opérateurs de communications électroniques, dont des URLs, des indices caractérisant la préparation d'un acte de terrorisme, telle qu'une succession de connexions révélant un comportement représentatif d'une menace.

- **Autorités administratives indépendantes**

  Administrations de l'État, mais disposant d'un statut garantissant l'indépendance de leurs membres à l'égard du Gouvernement, les autorités administratives indépendantes se voient confier par le législateur des missions spécialisées qu'il ne peut lui-même accomplir directement. Ces missions peuvent avoir pour but la protection des droits ou la régulation d'activités économiques. Dans le cas du renseignement, la CNCTR s'est vue confier par la loi la mission de contrôler la légalité de l'action des services de renseignement en matière de techniques de renseignement. Le statut et la liste des autorités administratives indépendantes ont été définis par la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.

## B

### Balisage

Cette technique de renseignement, prévue par l'article L. 851-5 du code de la sécurité intérieure, consiste à poser une « balise » au contact d'une cible pour localiser ses déplacements, ceux de son véhicule ou d'un objet lui appartenant.

## C

### Captation de paroles

Sonorisation de certains lieux ou enregistrement de paroles prononcées à titre privé ou confidentiel, selon les termes de l'article L. 853-1 du code de la sécurité intérieure qui prévoit l'autorisation d'y recourir.

Les dispositifs utilisés pour une telle captation, comme un micro, peuvent être installés dans un lieu privé : la procédure prévue pour obtenir l'autorisation de mettre en œuvre cette technique, identique à celle qui s'applique à la captation d'images dans un lieu privé ou au recueil de données informatiques, impose une délibération collégiale de la CNCTR, qui doit alors s'assurer que l'atteinte portée à la vie privée de la personne visée est strictement proportionnée à l'importance de la menace ou des enjeux concernés et que l'emploi de cette technique représente l'unique moyen d'obtenir les renseignements recherchés.

### Captation d'images

Prise de clichés photographiques ou enregistrement de bandes vidéos dans un lieu privé.

Les services de renseignement peuvent être autorisés, pour mettre en œuvre cette technique de renseignement prévue à

l'article L. 853-1 du code de la sécurité intérieure, à s'introduire dans un lieu privé.

Pour être autorisé à recourir à cette technique, un service doit convaincre la CNCTR, non seulement, que l'atteinte à la vie privée qui résulte de sa mise en œuvre est strictement proportionnée à l'importance de la menace ou des enjeux concernés, mais encore que cette technique représente bien l'unique moyen pour lui d'obtenir les renseignements recherchés.

- **Communication électronique internationale**

Communication électronique émise ou reçue à l'étranger.

Les communications concernées ne peuvent être interceptées que sur décision du Premier ministre, qui désigne alors les réseaux visés. Les communications interceptées peuvent ensuite être exploitées à des fins de surveillance pour l'ensemble des finalités prévues par la loi, si le Premier ministre, après avoir préalablement consulté la CNCTR, l'autorise.

- **Contenu**

L'accès au contenu d'une communication permet de connaître l'intégralité d'une correspondance : c'est la lettre contenue dans une enveloppe ou le message dans un courriel.

Cette notion s'oppose au contenant, telle l'enveloppe dans laquelle la lettre se trouve, qui, elle, ne révèle que l'identité et l'adresse de l'émetteur et du destinataire sans que puisse en être déduit le contenu de leur correspondance : c'est l'identifiant, le numéro de téléphone ou l'adresse de messagerie électronique d'une personne et de son correspondant.

- **Contingentement**

  Principe selon lequel le nombre d'autorisations simultanées de mise en œuvre d'une technique ne peut dépasser un quota fixé par le Premier ministre, après avis de la CNCTR. Cette limitation du nombre maximal de surveillances a pour but d'inciter les services à ne recourir à des techniques qu'en cas de nécessité et à mettre un terme aux autorisations devenues inutiles avant d'en solliciter de nouvelles. Elle s'applique notamment aux techniques, comme le recueil de données de connexion en temps réel et les interceptions de sécurité, dont la mise en œuvre peut porter, non seulement, sur des personnes surveillées à titre principal, mais également sur leur entourage. Leur contingentement permet ainsi de limiter au strict nécessaire le nombre de personnes susceptibles d'être visées.

- **Contrôle *a priori***

  La CNCTR contrôle la légalité de toutes les demandes de mise en œuvre de techniques de renseignement sur le territoire national, avant qu'elles ne soient soumises à l'autorisation du Premier ministre.

- **Contrôle *a posteriori***

  Pour garantir un contrôle complet et effectif de l'action des services de renseignement, le législateur a attribué à un organisme spécialisé, la CNCTR, des pouvoirs de vérification portant sur toutes les étapes de la procédure de mise en œuvre des techniques de renseignement : outre un examen préalable des demandes des services tendant à recourir à des techniques, la commission contrôle également la mise en œuvre des techniques autorisées : c'est le contrôle *a posteriori*.

# D

## Données de connexion

Informations permettant l'acheminement d'une communication électronique : elles sont assimilables à celles qui figurent sur l'enveloppe d'une lettre afin que celle-ci puisse parvenir à son destinataire, tels que le nom et l'adresse de l'émetteur et du destinataire.

Elles sont définies par l'article L. 851-1 du code de la sécurité intérieure comme des « *informations ou documents traités ou conservés* » par les « *réseaux* » ou les « *services de communications électroniques* » des opérateurs de communications électroniques, des hébergeurs et des fournisseurs de services sur internet, « *y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ».

Le recueil de ces données porte une atteinte moindre à la vie privée des personnes concernées que l'accès à leurs correspondances, c'est-à-dire au contenu de l'enveloppe. Les flux de communications électroniques sont tels, cependant, que l'accès aux données de connexion peut permettre de connaître ou de déduire de très nombreuses informations sur la vie privée de ces personnes, comme les habitudes de la vie quotidienne, les lieux de séjours ou les déplacements.

### Délégation parlementaire au renseignement

Instance parlementaire commune à l'Assemblée nationale et au Sénat dont la mission est de contrôler l'action du Gouvernement en matière de renseignement et d'évaluer la politique publique en ce domaine. Elle comprend huit membres, quatre députés et quatre sénateurs.

## E

### Extraction

Prélèvement, effectué à des fins d'analyse, d'une partie des données brutes recueillies lors de la mise en œuvre d'une technique de renseignement, telles que des images ou des paroles.

## F

### Fiches de traçabilité

Aux termes de l'article L. 822-1 du code de la sécurité intérieure (CSI), un relevé de mise en œuvre de chaque technique de renseignement, mentionnant « *les dates de début et de fin de mise en œuvre ainsi que la nature des renseignements collectés* », doit être établi. Ce relevé, plus couramment désigné sous le terme de « fiche de traçabilité », est « *tenu à la disposition de la commission qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement* ».

### Finalité

But de l'action d'un service de renseignement.

L'article L. 811-3 du code de la sécurité intérieure énumère de façon limitative celles qui peuvent légalement autoriser les

services de renseignement à recourir à ces techniques : leur objet est la défense ou à la promotion des d'intérêts fondamentaux de la Nation que la loi classe en sept catégories distinctes et limitatives.

- **Formation plénière**

  Formation du collège de la CNCTR comprenant tous ses membres, à savoir les quatre membres parlementaires, les quatre membres magistrats et la personnalité qualifiée dans le domaine des communications électroniques.

  Formation la plus solennelle de la Commission, elle se réunit au moins une fois par mois. Sa réunion est obligatoirement convoquée lorsque la CNCTR est saisie d'une demande de mise en œuvre d'une technique de renseignement visant une personne exerçant un mandat parlementaire ou la profession d'avocat, de journaliste ou de magistrat.

- **Formation restreinte**

  Formation du collège de la CNCTR comprenant les quatre membres exerçant les fonctions de magistrat et la personnalité qualifiée en matière de communications électroniques.

  Les demandes de mises en œuvre de techniques de renseignement impliquant la pénétration dans un lieu d'habitation ou le recueil de données informatiques dans un lieu privé nécessitent une délibération du collège réuni en formation restreinte.

## G

- **Groupement interministériel de contrôle**

  Service placé sous l'autorité du Premier ministre, le groupement interministériel de contrôle (GIC) a pour mission de centraliser l'ensemble des demandes de mise en œuvre

de techniques de renseignement, les autorisations de mise en œuvre délivrées par le chef du Gouvernement, l'exécution de certaines autorisations et les renseignements recueillis en application de ces autorisations.

Le GIC, qui n'est pas un service de renseignement, dispose du monopole des relations avec les opérateurs de communications électroniques pour la mise en œuvre de certaines techniques de renseignement, comme les interceptions de sécurité : il exécute les autorisations délivrées par le Premier ministre pour le compte de ces services et met à leur disposition les résultats de leur mise en œuvre.

- **Géolocalisation en temps réel**

  Dispositif de localisation en temps réel d'une personne sur une carte.

  Sa mise en œuvre, prévue à l'article L. 851-4 du code de la sécurité intérieure, consiste à localiser les équipements terminaux de communication d'une personne, comme un téléphone portable. Elle requiert le concours d'un opérateur de communications électroniques : celui-ci sollicite son réseau et transmet au groupement interministériel de contrôle, service du Premier ministre, les données obtenues.

- ***IMSI-catcher***

  Appareil de captation de proximité fonctionnant comme une antenne relai factice : son utilisation permet d'intercepter des données de connexion ou des correspondances échangées par des terminaux mobiles qui s'y sont connectés.

### Interception de sécurité

L'interception de sécurité, ou interception administrative de correspondances, permet d'écouter une conversation téléphonique ou de lire les correspondances écrites d'une personne, c'est-à-dire d'accéder au contenu de leurs communications. L'autorisation d'y recourir permet également d'accéder aux données de connexion correspondantes à ces communications.

### Intérêts fondamentaux de la Nation

Notion définie à l'article 410-1 du code pénal, les intérêts fondamentaux de la Nation « *s'entendent au sens (…) de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel* ».

Le législateur s'est inspiré de cette définition pour encadrer l'action des services de renseignement : la loi subordonne ainsi le recours à des techniques de renseignement à la défense ou la promotion des intérêts fondamentaux de la Nation, qu'elle a elle-même énumérés de façon limitative à l'article L. 811-3 du code de la sécurité intérieure. Les intérêts fondamentaux de la Nation pouvant permettre la mise en œuvre de techniques sont :

- L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

- Les intérêts économiques, industriels et scientifiques de la France ;
- La prévention du terrorisme ;
- La prévention des atteintes à la forme républicaine des institutions, la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous et la prévention des violences collectives de nature à porter gravement atteinte à la paix publique ;
- La prévention de la criminalité et de la délinquance organisées ;
- La prévention de la prolifération des armes de destructions massives.

## P

- **Police administrative**

  Mesures prises par une autorité administrative afin de prévenir, notamment, les troubles à l'ordre public ou les atteintes à la paix civile. La police administrative se distingue de la police judiciaire qui a, elle, pour finalité de réprimer la commission de telles atteintes.

- **Principe de proportionnalité**

  Principe selon lequel il doit exister une adéquation entre les moyens employés et le but visé.

  C'est en application de ce principe, notamment, que la CNCTR apprécie la légalité de la mise en œuvre des techniques de renseignement : elle s'assure que l'atteinte portée à la vie privée par l'emploi d'une technique est proportionnée à l'importance des menaces qu'elle vise à prévenir.

Pour les techniques les plus intrusives qui impliquent l'introduction dans un lieu privé, cette exigence de proportionnalité suppose en outre pour la commission d'effectuer un contrôle de subsidiarité : comme la loi le prévoit, elle doit alors vérifier, en application de ce principe, que les renseignements recherchés ne pourraient être efficacement collectés par d'autres moyens légaux moins attentatoires à la vie privée.

## Q

### Quorum

Toute question nouvelle ou sérieuse est renvoyée à la formation restreinte ou à la formation plénière. La formation restreinte et la formation plénière ne peuvent valablement délibérer que si, respectivement, au moins trois et quatre membres sont présents. Leurs décisions sont prises à la majorité des membres présents.

En cas de partage égal des voix, la voix du président est prépondérante (article L. 832-3 du CSI).

## R

### Recueil de données informatiques

Accès physique ou à distance à des données informatiques stockées dans un système informatique ou à des flux de données informatiques reçues, émises ou traitées par un tel système, dont des périphériques, comme un clavier, un écran d'ordinateur ou un micro.

La mise en œuvre de cette technique, prévue à l'article L. 853-2 du code de la sécurité intérieure, peut impliquer la pénétration d'agents des services dans un lieu privé, y compris à usage d'habitation.

La procédure prévue pour obtenir l'autorisation de mettre en œuvre cette technique, identique à celle qui s'applique à la captation de paroles ou d'images dans un lieu privé, impose une délibération collégiale de la CNCTR, qui doit s'assurer que l'atteinte portée à la vie privée de la personne visée est strictement proportionnée à l'importance de la menace ou des enjeux concernés et que l'emploi de cette technique représente l'unique moyen d'obtenir les renseignements recherchés.

- **Renseignement**

  Action préventive qui relève de la police administrative et à laquelle seuls les services de renseignement peuvent recourir : elle consiste à rechercher, collecter et analyser des informations relatives aux intérêts fondamentaux de la Nation, afin de les défendre ou de les promouvoir face à des menaces et à des risques susceptibles de les affecter.

  L'action des services de renseignement peut nécessiter le recours à des techniques attentatoires aux libertés, dont le droit au respect de la vie privée.

## S

- **Service de renseignement**

  Administration de l'État légalement compétente pour recourir à des techniques de renseignement.

- **Services spécialisés de renseignement – services du « premier cercle »**

  Au nombre de six, les services spécialisés de renseignement (DGSE, DGSI, DNRED, DRM, DRSD et Tracfin) ont reçu du législateur les missions de rechercher, collecter, exploiter et mettre à disposition du Gouvernement « *des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux*

*menaces et aux risques susceptibles d'affecter la vie de la Nation* ». La loi précise qu' « *ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces* ».

Dans ce cadre, ces services, à l'exception de la direction du renseignement militaire (DRM) et de Tracfin, ont vocation à recourir à toute la gamme des techniques de renseignement prévues par la loi, sous réserve que leur mise en œuvre corresponde à l'une au moins des sept finalités pouvant autoriser un tel recours.

- **Services du « second cercle »**

Communément appelés services du « second cercle », par opposition au « premier cercle » regroupant les services spécialisés de renseignement, ces services, dont le renseignement ne constitue qu'une partie des missions ou qui sont partie d'une administration dont la mission dépasse le seul renseignement, ne peuvent recourir qu'à **certaines des techniques de renseignement** prévues par la loi et pour un nombre limité de finalités.

Ils se trouvent au sein de la **direction générale de la police nationale**, de la **direction générale de la gendarmerie nationale**, de la **préfecture de police de Paris et de l'administration pénitentiaire**.

La plupart de ces services, soit près d'une vingtaine, n'exercent pas exclusivement une mission de renseignement : c'est le cas notamment des **services de police judiciaire**, comme la direction nationale de la police judiciaire, ou de certains **services territoriaux** ayant une mission généraliste, telles que les sections de recherche de la gendarmerie nationale.

Quatre d'entre eux, en revanche, se voient confier une mission exclusive de renseignement : il s'agit de la **direction nationale du renseignement territorial au sein de la direction générale de la police nationale**, de la **direction du renseignement de la préfecture de police de Paris**, de la sous-direction de l'anticipation opérationnelle au sein de la direction générale de la gendarmerie nationale et du **service national du renseignement pénitentiaire** au sein de la direction de l'administration pénitentiaire.

## T

### Technique de renseignement

Moyen de recueil du renseignement dont la mise en œuvre, faute d'autorisation donnée dans le cadre de la loi, constituerait une infraction pénale.

### Transcription

Action d'écrire sur un bulletin, à des fins d'analyse, ce que la mise en œuvre d'une technique a permis de voir ou d'entendre.

## U

### URL

L'URL, ou ***Uniform Resource Locator***, est une chaîne de caractères alphanumériques désignant l'adresse d'un contenu sur Internet, comme la page d'un site.

Ce type de données de connexion peut faire référence au contenu d'informations consultées par les utilisateurs d'Internet.

Ces données relèvent par conséquent à la fois des données de connexion, nécessaires pour l'acheminement d'une communication, et des données de contenu, car elles donnent des indications sur le contenu des informations consultées.

# 5. Dispositions du code pénal relatives à la réglementation « R. 226 »

## Partie législative

***LIVRE II : Des crimes et délits contre les personnes***

***Titre II : Des atteintes à la personne humaine***

***CHAPITRE VI DES ATTEINTES A LA PERSONNALITE***

***Section 1 De l'atteinte à la vie privée***

**Article 226-1 du code pénal**

Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.

Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient

opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale, dans le respect de l'article 372-1 du code civil.

Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, les peines sont portées à deux ans d'emprisonnement et à 60 000 euros d'amende.

Lorsque les faits sont commis au préjudice d'une personne dépositaire de l'autorité publique, chargée d'une mission de service public, titulaire d'un mandat électif public ou candidate à un tel mandat ou d'un membre de sa famille, les peines sont également portées à deux ans d'emprisonnement et à 60 000 euros d'amende.

**Article 226-3 du code pénal**

Est puni de cinq ans d'emprisonnement et de 300 000 € d'amende :

1° La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'Etat, lorsque ces faits sont commis, y compris par négligence, en l'absence

d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret ou sans respecter les conditions fixées par cette autorisation ;

2° Le fait de réaliser une publicité en faveur d'un appareil ou d'un dispositif technique susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le deuxième alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure lorsque cette publicité constitue une incitation à en faire un usage frauduleux.

Le présent article n'est pas applicable à la détention ou à l'acquisition par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, des appareils soumis à une autorisation du Premier ministre en application de la section 7 du chapitre II du titre Ier du livre II du code des postes et des communications électroniques.

### *Section 4 De l'atteinte au secret*

#### *Paragraphe 2 De l'atteinte au secret des correspondances*

**Article 226-15 du code pénal**

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie

électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.

Lorsqu'ils sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, ces faits sont punis d'une peine de deux ans d'emprisonnement et de 60 000 euros d'amende.

## Partie règlementaire

***LIVRE II : Des crimes et délits contre les personnes***

***Titre II : Des atteintes à la personne humaine***

***CHAPITRE VI DES ATTEINTES A LA PERSONNALITE***

***Section 1 De l'atteinte à la vie privée***

**Article R. 226-1 du code pénal**

La liste d'appareils et de dispositifs techniques prévue par l'article 226-3 est établie par arrêté du Premier ministre.

Par dérogation aux dispositions de l'article 1er du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles, les autorisations prévues aux articles R. 226-3 et R. 226-7 sont délivrées par le directeur général de l'Agence nationale de la sécurité des systèmes d'information.

**Article R. 226-2 du code pénal**

Il est institué auprès du Premier ministre une commission consultative composée comme suit :

1° Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant, président ;

2° Un représentant du ministre de la justice ;

3° Un représentant du ministre de l'intérieur ;

4° Un représentant du ministre de la défense ;

5° Un représentant du ministre chargé des douanes ;

6° Un représentant du ministre chargé de l'industrie ;

7° Un représentant du ministre chargé des télécommunications ;

8° Un représentant de la Commission nationale de contrôle des techniques de renseignement ;

9° Un représentant du directeur général de l'Agence nationale des fréquences ;

10° Deux personnalités choisies en raison de leur compétence, désignées par le Premier ministre.

La commission peut entendre, à titre d'expert, toute personne compétente.

Elle est saisie pour avis des projets d'arrêtés pris en application des articles R. 226-1 et R. 226-10. Elle peut formuler des propositions de modification de ces arrêtés.

Elle est également consultée sur les demandes d'autorisation présentées en application des articles R. 226-3 et R. 226-7.

Le secrétariat de la commission est assuré par l'Agence nationale de la sécurité des systèmes d'information.

**Article R. 226-3 du code pénal**

La fabrication, l'importation, l'exposition, l'offre, la location ou la vente de tout appareil ou dispositif technique figurant sur la liste mentionnée à l'article R. 226-1 est soumise à une autorisation, après avis de la commission mentionnée à l'article R. 226-2.

**Article R. 226-4 du code pénal**

La demande d'autorisation est déposée auprès du directeur général de l'Agence nationale de la sécurité des systèmes d'information. Elle comporte pour chaque type d'appareil ou de dispositif technique :

1° Le nom et l'adresse du demandeur, s'il est une personne physique, ou sa dénomination et son siège, s'il est une personne morale ;

2° La ou les opérations mentionnées à l'article R. 226-3 pour lesquelles l'autorisation est demandée et, le cas échéant, la description des marchés visés ;

3° L'objet et les caractéristiques techniques du type de l'appareil ou du dispositif technique, accompagnés d'une documentation technique ;

4° Le lieu prévu pour la fabrication de l'appareil ou du dispositif technique ou pour les autres opérations mentionnées à l'article R. 226-3 ;

5° L'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

**Article R. 226-5 du code pénal**

L'autorisation mentionnée à l'article R. 226-3 est délivrée pour une durée maximale de six ans.

Elle peut fixer les conditions de réalisation de l'opération et le nombre des appareils ou des dispositifs techniques concernés.

Elle est accordée de plein droit aux services de l'Etat désignés par arrêté du Premier ministre pour la fabrication d'appareils ou de dispositifs techniques.

**Article R. 226-6 du code pénal**

Chaque appareil ou dispositif technique fabriqué, importé, exposé, offert, loué ou vendu doit porter la référence du type correspondant à la demande d'autorisation et un numéro d'identification individuel.

**Article R. 226-7 du code pénal**

L'acquisition ou la détention de tout appareil ou dispositif technique figurant sur la liste mentionnée à l'article R. 226-1 est soumise à une autorisation, après avis de la commission mentionnée à l'article R. 226-2.

**Article R. 226-8 du code pénal**

La demande d'autorisation est déposée auprès du directeur général de l'Agence nationale de la sécurité des systèmes d'information. Elle comporte pour chaque type d'appareil ou de dispositif technique :

1° Le nom et l'adresse du demandeur, s'il est une personne physique, ou sa dénomination et son siège, s'il est une personne morale ;

2° Le type de l'appareil ou du dispositif technique et le nombre d'appareils ou de dispositifs techniques pour la détention desquels l'autorisation est demandée ;

3° L'utilisation prévue ;

4° L'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

**Article R. 226-9 du code pénal**

L'autorisation mentionnée à l'article R. 226-7 est délivrée pour une durée maximale de trois ans.

Elle peut subordonner l'utilisation des appareils ou des dispositifs techniques à des conditions destinées à en éviter tout usage abusif.

Elle est accordée de plein droit aux agents ou services de l'Etat pour l'acquisition et la détention des appareils ou dispositifs techniques qu'ils sont autorisés à utiliser en application de la loi.

**Article R. 226-10 du code pénal**

Les titulaires de l'une des autorisations mentionnées à l'article R. 226-3 ne peuvent proposer, céder, louer ou vendre les appareils ou dispositifs techniques figurant sur la liste prévue à l'article R. 226-1 qu'aux titulaires de l'une des autorisations mentionnées à l'article R. 226-3, à l'article R. 226-7 ou à l'article L. 34-11 du code des postes et communications électroniques.

Ils tiennent un registre retraçant l'ensemble des opérations relatives à ces matériels. Le modèle de ce registre est déterminé par arrêté du Premier ministre, pris après avis de la commission mentionnée à l'article R. 226-2.

**Article R. 226-11 du code pénal**

Les autorisations prévues à l'article R. 226-3 et à l'article R. 226-7 peuvent être retirées :

1° En cas de fausse déclaration ou de faux renseignement ;

2° En cas de modification des circonstances au vu desquelles l'autorisation a été délivrée ;

3° Lorsque le bénéficiaire de l'autorisation n'a pas respecté les dispositions de la présente section ou les obligations particulières prescrites par l'autorisation ;

4° Lorsque le bénéficiaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation.

Le retrait ne peut intervenir, sauf urgence, qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations.

Les autorisations prennent fin de plein droit en cas de condamnation du titulaire pour l'une des infractions prévues par les articles 226-1, 226-15 ou 432-9.

**Article R. 226-12 du code pénal**

Les personnes qui fabriquent, importent, détiennent, exposent, offrent, louent ou vendent des appareils ou des dispositifs techniques figurant sur la liste prévue à l'article R. 226-1 doivent se mettre en conformité avec les prescriptions de la présente section en sollicitant les autorisations nécessaires dans un délai de trois mois à compter de la publication de l'arrêté prévu à l'article R. 226-1.

Si l'autorisation n'est pas délivrée, ces personnes disposent d'un délai d'un mois pour procéder à la destruction de ces appareils ou dispositifs techniques ou pour les vendre ou les céder à une personne titulaire de l'une des autorisations prévues aux articles R. 226-3, R. 226-7 ou à l'article L. 34-11 du code des postes et communications électroniques. Il en est de même dans les cas d'expiration ou de retrait de l'autorisation.

***Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal***

**Article 1**

La liste prévue par l'article 226-3 du code pénal des appareils et des dispositifs techniques soumis à l'autorisation mentionnée à l'article R. 226-3 de ce code figure en annexe I au présent arrêté.

**Article 2**

La liste prévue par l'article 226-3 du code pénal des appareils et des dispositifs techniques soumis à l'autorisation mentionnée à l'article R. 226-7 de ce code figure en annexe II au présent arrêté.

**Article 3-1**

Le présent arrêté est applicable sur l'ensemble du territoire de la République.

**Article 4**

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information est chargé de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

### *Arrêté du 16 août 2006 relatif au registre visé par l'article R. 226-10 du code pénal*

**Article 1**

Le registre prévu à l'article R. 226-10 du code pénal retraçant l'ensemble des opérations relatives aux matériels dont la liste est fixée par l'arrêté du 29 juillet 2004 susvisé est conforme au modèle figurant en annexe du présent arrêté [*arrêté abrogé et remplacé par l'arrêté du 4 juillet 2012*].

**Article 2**

Ce registre revêt la forme d'un cahier coté et paraphé tenu par le responsable de la société qui a souscrit l'engagement de se soumettre aux contrôles nécessaires tel qu'il est prévu à l'article R. 226-4 du code pénal.

**Article 3**

L'arrêté du 15 janvier 1998 ayant le même objet est abrogé.

**Article 4**

Le présent arrêté sera publié au Journal officiel de la République française.

*Photos crédits : H. Véronèse/Centre Pompidou/Patrick Gaillardin/Léo-Paul Ridet/Sorbonne Université/Florian Guigui.*


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

Maquette : DSAF / DPSG / BAEC / Section Édition – Impression : Baudelaire - juin 2025 - ISSN 2966-9421.