CNCTR

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

8e Rapport d'activité 2023

Avant-propos

Le renseignement contre le crime…

21 000 personnes surveillées en France en 2022. 24 000 en 2023. Cette progression était sans doute attendue dans son principe. Elle est la conséquence de l'aggravation des menaces qui pèsent sur notre pays. Son analyse en termes de finalités de la surveillance ménage toutefois quelque surprise.

Certes, les tensions internationales multiples conduisent à une augmentation sensible des personnes surveillées au titre de la contre-ingérence. De même, la résurgence d'un risque terroriste sur le territoire national alliée à la dissémination des auteurs potentiels, souvent des individus jeunes et isolés, explique la multiplication du nombre des « cibles ».

Mais l'évolution la plus marquante ne relève d'aucune de ces deux finalités. C'est la progression du nombre des personnes suivies au titre de la prévention de la délinquance et de la criminalité organisées. Pour la première fois, c'est une finalité autre que la prévention du terrorisme qui devient la première des finalités en nombre de cibles. L'importance de cette intervention de la police administrative dans un domaine qui appartenait traditionnellement à la police judiciaire montre que la menace liée au trafic de stupéfiants est désormais devenue un enjeu pour le fonctionnement normal des institutions.

Une inévitable escalade dans les techniques de surveillance

Le nombre des demandes adressées à la commission pour la mise en œuvre de techniques de renseignement a continué de croître : 95 000 demandes en 2023. Cette augmentation (+ 6 % par rapport à l'année précédente) est toutefois inférieure à celle du nombre des personnes surveillées. En effet, la surveillance administrative au titre de la prévention de la criminalité organisée est plus ramassée dans le temps et moins consommatrice de techniques que lorsqu'il

s'agit de surveiller une filière terroriste : dès que les soupçons sont confirmés, c'est à l'autorité judiciaire de prendre la main.

La commission y veille.

Plus significatif que cette augmentation limitée en volume est le recours toujours croissant aux techniques les plus intrusives. Pose de micros dans des lieux privés, recueil de l'ensemble des données informatiques de la personne, piégeage des téléphones et des ordinateurs : on s'efforce ainsi de compenser le désormais faible apport des écoutes téléphoniques. Cette forme d'escalade paraît difficilement résistible, les personnes surveillées (notamment celles pratiquant des formes d'extrémisme violent) étant de plus en plus conscientes du risque d'une surveillance technique et aptes à s'en prémunir. Il convient donc de l'encadrer strictement.

Or, à la différence des écoutes téléphoniques, centralisées par un service de Matignon (le groupement interministériel de contrôle, GIC), ces techniques spécialement intrusives sont directement mises en œuvre par les services demandeurs. Leur produit est conservé et exploité dans les systèmes de ces mêmes services. Il est difficilement accessible à la commission, la loi n'ayant pas prévu son accès direct à ces systèmes, à la différence de ce qui vaut pour les données conservées par le GIC. Par ailleurs, sa maîtrise est complexe, les données captées étant volumineuses et hétérogènes.

Le risque est alors celui d'un affaiblissement progressif du contrôle.

Vers un meilleur contrôle

La commission avait fortement souligné ce risque dans son précédent rapport. Elle a été entendue. Sur instruction du Président de la République au Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), un travail commun a été mené entre les directions techniques de la direction générale de la

sécurité extérieure (DGSE) et de la direction générale de la sécurité intérieure (DGSI). L'objectif est qu'en 2027, le GIC soit en mesure de centraliser l'ensemble des données issues de la technique de recueil des données informatiques, jouant ainsi pleinement son rôle de « tiers de confiance ». La commission pourra y accéder facilement à distance, pour les besoins de son contrôle, de même que les services, pour en exploiter le contenu.

La commission se réjouit de cet important pas en avant. Il s'ajoute à un ensemble de progrès réalisés avec l'aide des services dans la facilitation matérielle du contrôle, notamment en matière de surveillance internationale. Ces progrès viennent en complément des échanges avec les services, sans s'y substituer : la dimension humaine du contrôle, les échanges qu'elle permet demeurent irremplaçables pour la commission.

Faire vivre l'État de droit…

L'État de droit n'est pas un état donné une fois pour toutes. C'est une tension, une quête, qui réclame des ajustements permanents du droit à la réalité des choses. Il n'en va pas différemment pour le contrôle du renseignement. Ainsi, le rendez-vous législatif de 2025[1] peut être l'occasion de parfaire un cadre législatif qui a, pour l'essentiel, fait ses preuves. La commission a cru utile, dans un souci de bonne administration, d'apporter sa contribution à la préparation de ce rendez-vous en signalant dans le présent rapport un ensemble de points qui pourraient justifier une intervention du législateur. Je souligne ici ceux d'entre eux qui permettraient de progresser dans la garantie des droits.

La manière dont est aménagé le droit au recours pour les personnes craignant d'être surveillées sans raison légitime est perfectible. La loi prévoit certes que la commission, saisie par toute personne, vérifie

1. Voir partie 3.2 du rapport ci-dessous.

qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard. Le nombre de ces réclamations a presque doublé en 2023. Mais la capacité de « vérification » de la commission se heurte à l'interdiction qui lui est faite, selon une interprétation d'ailleurs contestable de la loi, d'accéder aux fichiers dits « de souveraineté », y compris en tant que ces derniers sont susceptibles de permettre de capitaliser les résultats de techniques de renseignement. La vérification est donc incomplète.

Le réclamant insatisfait a certes la faculté de saisir le Conseil d'État d'un recours contentieux. Toutefois, les explications données au juge par les services du Premier ministre et la commission étant couvertes par le secret de la défense nationale, le requérant n'a pas accès au dossier. Il n'apparaît pourtant pas impossible de trouver des accommodements entre protection du secret et respect du caractère contradictoire de la procédure juridictionnelle, par exemple en s'inspirant de la procédure britannique et en permettant au requérant de faire appel à un avocat qui serait choisi parmi un tout petit nombre d'avocats spécialement habilités.

On rappellera également la question du contrôle des échanges de données entre les services français et leurs homologues étrangers, contrôle que l'on sait nécessaire pour répondre aux exigences de la Cour européenne des droits de l'homme, mais dont on diffère, d'année en année, la traduction législative, dans l'attente d'une décision de la Cour concernant le cadre légal français, décision dont on ignore à la fois quand elle interviendra, et si elle traitera de ce sujet…

Enfin, à un très proche horizon, apparaît l'enjeu de l'intelligence artificielle. Un outil dont le renseignement ne saurait se passer. Et un défi pour le régulateur, qui se demande déjà si la surveillance d'une personne en viendra à être décidée selon des critères dont aucun humain ne connaîtra ni la teneur ni la pondération de façon certaine… Aussi a-t-il paru légitime que la commission apporte sa contribution particulière au flot actuel des réflexions. C'est l'objet d'une étude que

l'on trouvera dans la partie « Éclairages » de ce rapport. Dans le même esprit, cette partie accueille une contribution de l'ambassadeur pour le numérique, qui évoque les efforts de la France à l'international pour la nécessaire régulation des dispositifs de cyber-intrusion.

… et donner de la sécurité juridique aux services

Il est normal et nécessaire que le cadre légal reçoive des ajustements, soit à l'occasion d'une modification législative, soit du fait d'une évolution de la doctrine de la commission sur les conditions d'application de la loi. Mais les services de renseignement, à la façon des entreprises, ont aussi besoin de bénéficier de ce que les juristes appellent la sécurité juridique : les positions de la commission doivent être facilement accessibles, clairement exposées et bien diffusées ; les changements doctrinaux doivent être suffisamment prévisibles ; leur impact doit être apprécié par un échange préalable avec les services intéressés.

La commission s'est pleinement engagée dans la mise en œuvre de ces principes. Elle a enrichi le dialogue avec les services, à la fois pour mieux caractériser les menaces, apprécier précisément le bien fondé des demandes, être éclairée sur les effets de certaines positions qu'elle se propose d'adopter. Elle a aussi consolidé sa doctrine et préparé un système de diffusion adapté. Elle a trouvé, au sein des différents services, des interlocuteurs ouverts à un dialogue constructif.

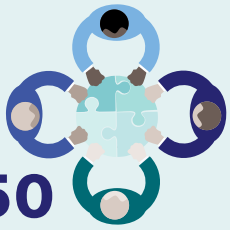
Il y a lieu d'espérer que la diminution, en 2023, de la part des avis défavorables rendus sur les demandes de techniques (1,2 % contre 1,6 % l'année précédente) est au moins pour partie le résultat de cette démarche.

Serge LASVIGNES
Conseiller d'État honoraire
Président de la CNCTR

Les chiffres clés de l'année

94 902
demandes de techniques de renseignement
(domestiques)

24 209
personnes surveillées



150
réunions collégiales

136
contrôles
dans les services

3,1 millions €
de budget

2023

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

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

20
agents
(au 31/12/2023)

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

Rapport d’activité 2023

Partie 1. L'état de la surveillance en 2023 : une hausse du nombre des personnes surveillées et des techniques mises en œuvre en lien avec le renforcement de certaines menaces

Comme dans ses précédents rapports, la Commission nationale de contrôle des techniques de renseignement (CNCTR) rend compte 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, en publiant des informations aussi détaillées que le permet le secret de la défense nationale sur son activité de contrôle et en livrant au public 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.

La commission rend par ailleurs compte du nombre d'avis préalables qu'elle a rendus en 2023 sur les demandes relevant de la surveillance des communications électroniques internationales.

1. Les dispositions de l'article L. 811-3 du code de la sécurité intérieur 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* » (finalité 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* ».

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.

1.1. Une hausse marquée 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 calculé le nombre de personnes ayant fait l'objet en 2023 d'au moins une technique de renseignement, parmi celles prévues aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure. 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 diminué de près de 9 % en 2022, le nombre de personnes surveillées s'élève cette année à 24 209 soit une augmentation de plus de 15 % par rapport à l'année 2022, et de 9 % par rapport à la période antérieure à la crise sanitaire liée à la pandémie de Covid-19.

2. La CNCTR considère en effet que les identifications d'abonnés et les recensements de numéros d'abonnement, prévus au deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, 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.

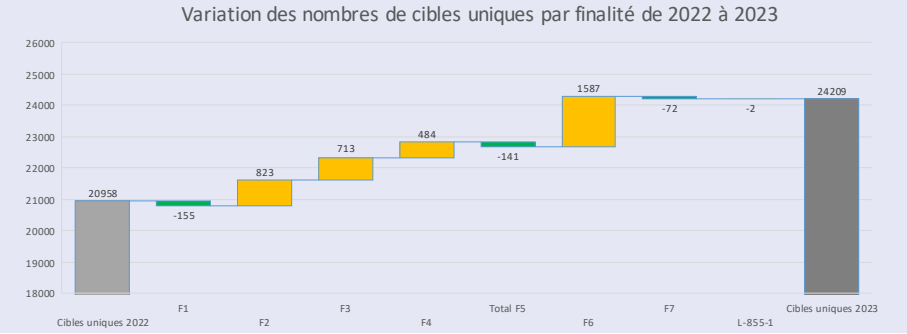
	2019	2020	2021	2022	2023	Evolution 2022/2023	Evolution 2019/2023
Nombre de personnes surveillées	**22 210**	**21 952**	**22 958**	**20 958**	**24 209**	**+ 15,5 %**	**+ 9 %**
Au titre de la prévention du terrorisme	**7 736** (34,8 % du total)	**8 786** (40 % du total)	**7 826** (34,1 % du total)	**6 478** (30,9 % du total)	**6 962** (28,8 % du total)	**+ 7,5 %**	**- 10 %**
Au titre de la prévention de la criminalité et de la délinquance organisées	**5 693** (25,6 % du total)	**5 021** (22,9 % du total)	**5 932** (25,8 % du total)	**5 471** (26,1 % du total)	**7 058** (29,2 % du total)	**+ 29 %**	**+ 24 %**
Au titre de la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure[3]	**3 021** (13,6 % du total)	**3 238** (14,8 % du total)	**3 466** (15,1 % du total)	**2 692** (12,8 % du total)	**2 551** (10,5 % du total)	**- 5,2 %**	**- 15,6 %**

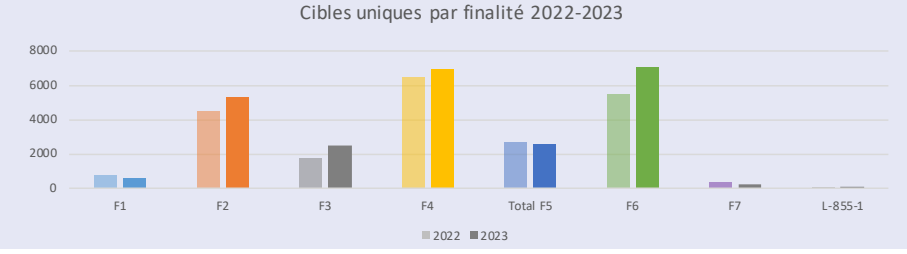
Cette augmentation du nombre de personnes surveillées est à mettre en lien avec l'évolution de la menace en nature comme en intensité. Elle a principalement pour origine un investissement inédit dans la prévention de la délinquance et de la criminalité organisées ainsi qu'un renforcement de la lutte contre les diverses formes d'ingérence (1.1.1). En revanche, 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 deuxième année de suite une légère diminution (1.1.2).

3. C'est-à-dire 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.

1.1.1. Une forte hausse du nombre de personnes surveillées en corrélation avec l'évolution de l'état de la menace : la prévention de la délinquance et de la criminalité organisées devient le premier motif de surveillance en nombre de personnes concernées

Les graphiques ci-dessous permettent de visualiser à la fois la manière dont se répartit l'augmentation du nombre de personnes surveillées entre les différentes finalités[4] et l'évolution de ce nombre pour chacune de ces finalités entre 2022 et 2023.





(F1) : finalité 1, 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.

4. Il y a lieu de souligner qu'une même personne pouvant être surveillée au titre de plusieurs finalités, le différentiel total constaté entre 2022 et 2023 ne correspond pas à l'agrégation des différentiels constatés finalité par finalité.

Les données de l'année 2023 mettent d'abord en évidence une augmentation d'un peu plus de 29 % du nombre de personnes surveillées au titre de **la prévention de la criminalité et de la délinquance organisées** (finalité 6). Cette forte augmentation peut s'expliquer à la fois par une maîtrise croissante des techniques par les services spécialisés et par leur effort accru, notamment en ce qui concerne la lutte contre le trafic de stupéfiants, devenue en quelques années un enjeu majeur en termes de sécurité publique. L'augmentation relevée en 2023 s'inscrit dans le cadre d'une augmentation de 24 % du nombre de personnes surveillées au titre de cette finalité depuis 2019 (+ 42 % depuis 2016)[5]. Au-delà, l'ampleur de l'enjeu ressort également du fait que cette année, plus de personnes ont été surveillées au titre de cette finalité qu'au titre de la prévention du terrorisme.

En ce qui concerne la finalité tenant à **la prévention du terrorisme** (finalité 4), le nombre de personnes surveillées a augmenté de 7,5 % au cours de l'année 2023 en corrélation avec la résurgence des risques tant exogènes qu'endogènes dans un contexte international très instable ; la survenance d'attentats sur le territoire national contraignant les services de renseignement à réévaluer l'état de la menace.

Même si la tendance générale est à la baisse sur une période plus longue (- 10 % de personnes surveillées par rapport à 2019, - 22 % par rapport à 2016[6]), l'augmentation constatée en 2023 met en évidence la résurgence de la menace en la matière ainsi que son caractère protéiforme, celle-ci étant de plus en plus liée à des individus isolés, pouvant passer à l'acte de façon précipitée et dont le suivi ou la reprise du suivi a une incidence sur l'activité des services.

5. 4 969 personnes étaient surveillées au titre de la prévention de la criminalité et de la délinquance organisées en 2016, représentant 24,4 % du total des personnes surveillées la même année. Voir le 2ème rapport d'activité 2017 de la CNCTR, p. 54.

6. 9 475 personnes étaient surveillées au titre de la prévention du terrorisme en 2016, représentant 46,5 % du total des personnes surveillées la même année. Voir le 2ème rapport d'activité 2017 de la CNCTR, p. 54.

L'instabilité du contexte international, à travers en particulier la guerre en Ukraine depuis l'année 2022 et la réactivation du conflit israélo-palestinien au second semestre 2023, est également de nature à expliquer l'augmentation du nombre de personnes surveillées au titre de la **finalité tenant aux 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).

Enfin, le nombre de personnes surveillées au titre de la **défense et de la promotion des intérêts économiques, industriels et scientifiques majeurs de la France** (finalité 3) est également en augmentation mais retrouve ce faisant le niveau constaté en 2019[7] avant le déclenchement de la crise sanitaire

S'agissant de ces deux dernières finalités, cette tendance légèrement haussière est conforme à celle déjà observée l'année dernière.

1.1.2. Une baisse du nombre de personnes surveillées au titre de la prévention des extrémismes violents et des violences collectives qui se confirme

À l'instar de la tendance relevée en 2021 et en 2022, le recul du nombre de personnes surveillées au titre de la finalité prévue au 5° de l'article L. 811-3 du code de la sécurité intérieure se confirme avec une baisse de 5,2 % par rapport à 2022. Le nombre de personnes surveillées au titre de cette finalité atteint ainsi son plus bas niveau depuis 2018[8].

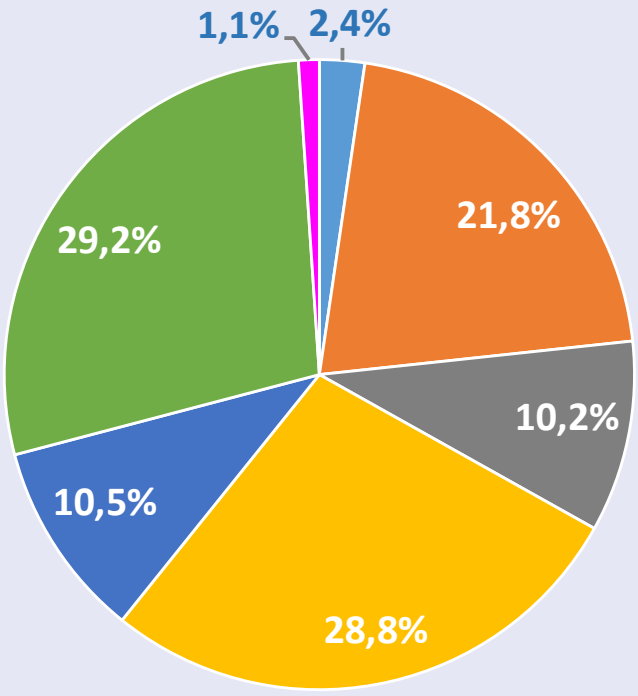
7. Voir 4ème rapport d'activité 2019 de la CNCTR p. 57 et suivantes.

8. 2 116 personnes étaient surveillées au titre de la finalité mentionnée au 5° de l'article L. 811-3 du code de la sécurité intérieure en 2018. Voir le 6ème rapport d'activité 2021 de la CNCTR, p. 73.

Cette évolution, qui s'accompagne d'une tendance à la baisse du taux d'avis défavorables rendus par la commission sur les demandes de techniques, est sans doute à mettre en lien avec la démarche menée par la commission, au cours de l'année 2023, afin de mieux expliquer les contours de cette finalité et de mieux diffuser sa doctrine notamment à travers l'étude thématique consacrée à la matière dans le cadre de son précédent rapport d'activité, dont une version classifiée a été adressée aux services. Cette initiative a permis d'instaurer un dialogue particulièrement constructif avec ces derniers qui a conduit à un ciblage plus précis des personnes d'intérêt[9].

9. 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



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

MÉTHODOLOGIE DE CALCUL DU NOMBRE DE PERSONNES SURVEILLÉES

Le calcul du nombre de personnes surveillées est assuré par la CNCTR à l'aide des données communiquées par le GIC. Ces données sont issues des différents traitements informatisés permettant de traiter les demandes de techniques de renseignement en se fondant sur celles pour lesquelles une autorisation du Premier ministre a été accordée durant l'année de l'étude.

Les résultats de ce calcul comportent toutefois une marge d'erreur eu égard à différentes contraintes.

En effet, 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, même si l'année 2023 a permis d'améliorer cette harmonisation s'agissant des géolocalisations en temps réel[10]. Par ailleurs, les demandes des services sont formées 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.

Pour pallier le risque de « doublon » résultant de ces différentes contraintes techniques et opérationnelles, la commission a développé une approche algorithmique fondée sur la comparaison des éléments présents dans les demandes de techniques telles que les informations liées à l'état civil de la personne ciblée mais aussi les identifiants rattachés aux équipements visés par la technique de renseignement (par exemple le numéro de téléphone mis sous interception de sécurité). Ces comparaisons permettent d'identifier les personnes qui apparaissent sous plusieurs identifiants dans les différentes bases mises à disposition par le GIC pour le calcul et d'éliminer les « doublons ».

Au final, l'indicateur calculé, soit le nombre de cibles surveillées, comporte une marge d'erreur que la CNCTR estime à moins de 10 %. Toutefois, la commission travaille actuellement à des évolutions possibles de sa méthode de calcul afin de renforcer la fiabilité des résultats obtenus.

10. Technique de renseignement prévue par l'article L. 851-4 du code de la sécurité intérieure.

1.2. Une augmentation continue du nombre des techniques de surveillance demandées

En 2023, le volume total de demandes tendant à la mise en œuvre de techniques de renseignement sur le territoire national est supérieur de 6 % à celui enregistré en 2022. Cette augmentation est très inférieure à celle du nombre de personnes surveillées (+ 15 %). Le différentiel de croissance s'explique sans doute largement par le fait que l'augmentation du nombre de personnes surveillées est principalement due à la prévention de la délinquance organisée. En effet, la surveillance en la matière est plus courte : soit elle est infructueuse et est arrêtée (ou non renouvelée), soit elle débouche rapidement sur une saisine de l'autorité judiciaire. En outre, les services qui en ont principalement la charge font moins appel à des techniques multiples (hors prestations d'identification, le nombre moyen de techniques sollicitées par personne surveillée au titre de cette finalité est de l'ordre de 1,6 alors qu'il est de 3 au titre de la finalité tenant à la prévention du terrorisme).

On rappellera que 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 sa décision[11]. Elle doit se prononcer dans un délai de vingt-quatre heures lorsqu'une demande relève de la compétence d'un membre ayant la qualité de magistrat[12] et statuant seul. Ce délai est porté à soixante-douze heures lorsque cette demande nécessite un examen en formation collégiale, plénière ou restreinte[13]. La CNCTR s'attache à respecter ces délais.

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

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

13. 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.

Par ailleurs, comme l'expliquait le précédent rapport d'activité de la commission, une procédure dite « prioritaire » a été mise en place pour répondre aux besoins opérationnels nécessitant un traitement urgent des demandes. Elle permet de rendre des avis dans un délai généralement inférieur à une heure[14].

1.2.1. Les avis rendus en matière de surveillance intérieure : la confirmation d'un recours accru aux techniques les plus intrusives

En matière de surveillance intérieure, les avis émis par la CNCTR 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 2019 à 2023. Ils permettent de saisir les évolutions sur 5 ans et d'une année sur l'autre, de la façon dont les services recourent à chaque catégorie de techniques.

	2019	2020	2021	2022	2023	Évolution 2023 / 2023	Évolution 2019 / 2023
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)	25 051	30 758	32 254	31 427	33 657	+ 7,1 %	+ 34,4 %
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)	14 568	18 006	19 974	19 263	21 430	+ 11,2 %	+ 47,1 %
Accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure)	1 184	1 644	1 534	1 175	763	- 35,1 %	- 35,6 %

14. Voir sur ce point le 7ème rapport d'activité 2022, p. 16-17.

	2019	2020	2021	2022	2023	Évolution 2023 / 2023	Évolution 2019 / 2023
Géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure)	7 601	8 394	9 920	10 901	10 982	+ 0,7 %	+ 44,5 %
Interceptions de sécurité via le GIC (I de l'article L. 852-1 du code de la sécurité intérieure)	12 574	12 891	12 736	12 798	13 021	+ 1,7 %	+ 3,6 %
Interceptions des communications par *IMSI catcher*[15] (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)	3	0	3	5	10	+ 100 %	+ 233,3 %
Interceptions de correspondances émises ou reçues par la voie satellitaire (article L. 852-3 du code de la sécurité intérieure)	0	0	0	0	0	-	-
Localisations des personnes ou des objets (« Balisages ») (article L. 851-5 du code de la sécurité intérieure)	1 793	1 598	2 006	1 951	2 084	+ 6,8 %	+ 16,2 %
Recueils de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure)	288	311	583	641	607	- 5,3 %	+ 110,8 %
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)	3 282	1 564	2 138	3 314	3 802	+ 14,7 %	+ 15,8 %
Recueils et captations de données informatiques (article L. 853-2 du code de la sécurité intérieure)	3 591	2 418	3 758	4 260	4 493	+ 5,5 %	+ 25,1 %
Introductions dans des lieux privés (article L. 853-3 du code de la sécurité intérieure)	3 599	2 021	2 682	3 767	4 053	+ 7,6 %	+ 12,6 %
Ensemble des techniques de renseignement	73 534	79 605	87 588	89 502	94 902	+ 6 %	+ 29,1 %

15. Il s'agit de dispositifs techniques permettant de capter des données de connexion des équipements terminaux, notamment le numéro de leur carte SIM ou IMSI (*International mobile subscriber identity*).

Ces données font apparaître qu'après avoir augmenté de façon modérée en 2022 (+ 2,2 %), le nombre total de demandes tendant à la mise en œuvre de techniques de renseignement enregistre donc en 2023 une hausse de 6 %, plus proche des évolutions annuelles de 2020 et 2021.

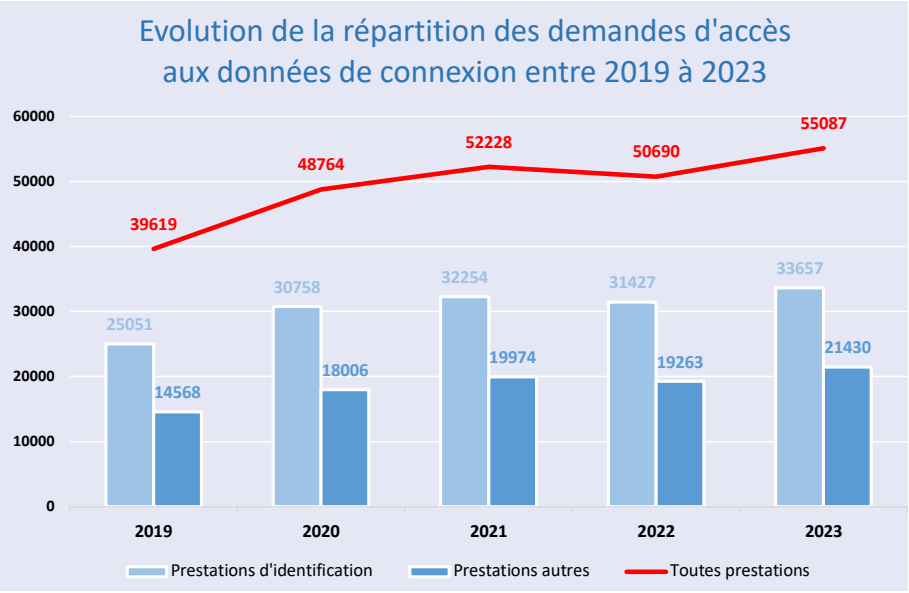
À l'exception de l'accès aux données de connexion en temps réel et du recueil de données de connexion par *IMSI-catcher*, cette augmentation concerne, dans des proportions plus ou moins marquées, toutes les techniques de renseignement relevant du code de la sécurité intérieure.

Les accès aux données techniques de connexion demeurent très largement la technique de surveillance de première intention.

À l'instar des années précédentes, **les demandes d'accès aux données de connexion en temps différé**, qui présentent un moindre caractère intrusif par rapport aux autres techniques, demeurent les techniques de référence. Elles affichent en 2023 une hausse de 9 % après avoir connu une baisse en 2022.

Cette tendance haussière résulte de l'augmentation du nombre de personnes faisant l'objet d'une surveillance, ces techniques constituant en quelque sorte des techniques de première intention. Elle s'explique également par la diversification des prestations demandées au GIC, incluant désormais notamment les données liées à l'utilisation des réseaux sociaux.

Il convient de rappeler qu'en application de la méthode de comptabilisation de la commission, une demande est susceptible de porter sur plusieurs accès à la fois. Ainsi, une demande de recensement de numéros d'abonnement téléphonique d'une personne peut entraîner le recueil de plusieurs numéros auprès de plusieurs opérateurs de communications électroniques et, partant, l'émission de plusieurs réquisitions.



En revanche, les **demandes d'accès aux données de connexion en temps réel**, qui avaient connu de fortes hausses en 2019 et 2020, continuent de fortement diminuer : - 35 % cette année, après un recul de 23 % en 2022. Ce plus faible recours à cette technique résulte peut-être du fait qu'elle est, en vertu des dispositions de l'article L. 851-2 du code de la sécurité intérieure, cantonnée à la finalité tenant à la prévention du terrorisme.

Les techniques de surveillance dont le caractère intrusif peut être qualifié d'intermédiaire augmentent de façon modérée.

Ainsi, les demandes de **géolocalisation en temps réel** ont vu leur nombre se stabiliser au cours de l'année 2023 (+ 0,7 %), après cinq années de croissance, matérialisée par une hausse de 45 % entre 2019 et 2023. Cette technique, permettant une surveillance des déplacements de la cible sans mobiliser physiquement des agents, est également une technique de référence désormais bien connue et maîtrisée par les services.

Les demandes **d'interceptions de sécurité** (les « écoutes ») réalisées *via* le GIC s'inscrivent pour la cinquième année consécutive également dans une relative stabilité. Ainsi, 13 021 demandes ont été présentées en 2023, contre 12 798 en 2022 (+ 1,7 %).

Cette faible augmentation peut sans doute être attribuée au contingentement de la technique prévue par l'article L. 852-1 du code de la sécurité intérieure qui n'a pas connu d'évolution au cours de l'année 2023. Elle s'explique aussi probablement par une forme d'autorégulation des services au regard des ressources qui doivent être engagées pour exploiter ces interceptions.

L'utilisation des techniques de localisation des personnes ou des objets (les « balises ») reste stable sur les trois dernières années, soit un volume de l'ordre de 2 000 demandes par an.

Les techniques de surveillance les plus intrusives poursuivent une progression soutenue.

Les techniques de **captation de paroles prononcées à titre privé ou de captation d'images dans un lieu privé**, continuent ainsi d'augmenter sensiblement. Si on fait abstraction de la baisse drastique des années 2020 et 2021 liée à la pandémie de Covid 19, on constate qu'entre 2019 et 2023, les demandes portant sur ces techniques ont augmenté de près de 16 %. Il est clair que cette évolution est en relation directe avec la moindre productivité des écoutes téléphoniques liée à l'usage des messageries cryptées ou sécurisées.

Selon la même logique, **la technique de recueil et de captation des données informatiques** (RDI) a également connu une augmentation notable en 2023 (+ 5,5 %) moins importante il est vrai que celle constatée en 2022 (+ 13,4 %). Sur la période 2019-2022, cela représente une hausse du recours à cette technique supérieure à 25 %.

Par ailleurs, 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 code de la sécurité intérieure) a été accordée en 2023, portant à cinq le nombre d'algorithmes autorisés depuis l'ouverture de cette technique aux services de renseignement en 2015. 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)[16] n'a toutefois pas encore été mise en œuvre.

En revanche, les **recueils de données de connexion par *IMSI catcher*** ont été moins nombreux en 2023 avec 607 demandes, contre 641 en 2022, représentant une baisse de 5,3 %. Cette baisse est néanmoins à relativiser au regard de l'importante augmentation du recours à la technique (+ 110 %) sur l'ensemble de la période 2019-2023.

La diminution du recours aux *IMSI catcher* en 2023 est principalement due aux contraintes opérationnelles qu'implique la mise en œuvre efficace des appareils ou dispositifs techniques concernés.

1.2.2. Une augmentation du nombre de demandes d'autorisation d'exploitation en matière de surveillance des communications électroniques internationales

En 2023, la commission a rendu 3 981 avis sur des demandes tendant à l'exploitation de communications internationales interceptées, contre 3 715 en 2022, soit une hausse de 7 %. L'évolution du nombre des avis rendus par la CNCTR sur les demandes de surveillance

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

des communications électroniques internationales sur la période 2019-2022 est détaillée dans le tableau ci-dessous.

	2019	2020	2021	2022	2023	Évolution 2023 / 2023	Évolution 2019 / 2023
Nombre d'avis rendus en matière de surveillance des communications électroniques internationales	**2 133**	**4 316**	**4 374**	**3 715**	**3 981**	**+ 7,2 %**	**+ 86,6 %**

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. 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 code de la sécurité intérieure 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.

1.2.3. Un nombre d'avis défavorables néanmoins en baisse à la faveur d'un dialogue amélioré avec les services

De façon de prime abord contre-intuitive, la hausse du nombre des personnes surveillées et du nombre des demandes de techniques de renseignement n'a pas conduit à une augmentation des avis défavorables rendus par la commission. Au contraire, le nombre des avis défavorables connaît une baisse sensible de 20 % (775 avis défavorables contre 974 en 2022), toutes techniques confondues, par rapport à l'année 2022. Hors demandes de données de connexion, le taux d'avis défavorables représente ainsi 1,2 % du total des demandes contre 1,6 % en 2022.

Ce résultat s'explique sans doute par les progrès dans la maîtrise du cadre légal, avec un important travail de formation mené par les services et une politique de consolidation et de diffusion de sa doctrine par la commission. Il est aussi lié à un développement des échanges entre la commission et les services soit avant la transmission d'une demande estimée délicate, soit lors de son instruction, à l'initiative de la commission.

Dans ses rapports d'activité de 2019 et 2022[17], la CNCTR a expliqué comment elle a enrichi la procédure d'instruction des demandes prévue par la loi en se réservant la possibilité d'inviter les services à compléter la motivation de leurs demandes afin d'apprécier plus aisément à la fois la nécessité et la proportionnalité des moyens sollicités par rapport à l'intérêt que présente la personne visée.

Ces demandes de renseignements complémentaires peuvent porter aussi bien sur le fond des dossiers que sur la mise en œuvre concrète des techniques envisagées, de façon à lever toute ambiguïté et de mesurer pleinement l'impact des mesures envisagées sur les personnes ciblées ou leur environnement proche.

17. Voir notamment le 7ème rapport d'activité 2022 de la CNCTR, p. 28 et suivantes.

Cet outil très important dans le cadre du contrôle *a priori* permet de distinguer plus aisément les demandes dont la motivation est insusceptible de respecter le cadre d'emploi des techniques prévu par la loi de celles dont la rédaction est imprécise ou équivoque.

Or, alors que le nombre de ces demandes de renseignements complémentaires avait très sensiblement augmenté en 2022, cette augmentation s'est poursuivie à un niveau élevé en 2023 avec une augmentation de plus 21 % s'agissant des techniques autres que les recueils de données de connexion.

	2022	2023	Évolution 2022 / 2023
Techniques de renseignement (hors données techniques de connexion)			
Avis rendus	**38 830**	**39 848**	**2,6 %**
Demandes de renseignements complémentaires	**1 134** (soit 2,9 % du total)	**1 373** (soit 3,4 % du total)	**+ 21,1 % (0,5 pt)**
Avis défavorables	**629** (soit 1,6 % du total)	**496** (soit 1,2 % du total)	**- 21,1 % (-0,4 pt)**
Toutes techniques de renseignement confondues			
Avis rendus	**89 520**	**94 935**	**6,0 %**
Demandes de renseignements complémentaires	**2 582** (soit 2,9 % du total)	**2 797** (soit 2,9 % du total)	**+ 8,3 % (0 pt)**
Avis défavorables	**974** (soit 1,1 % du total)	**775** (soit 0,8 % du total)	**- 20,4 % (-0,3 pt)**

UNE MÉTHODE DE TRAVAIL AXÉE SUR L'ÉCHANGE ET LA COMMUNICATION

Le dialogue avec les services est primordial pour la compréhension mutuelle et la mise en œuvre d'un contrôle pertinent et efficace.

Si les demandes de renseignements complémentaires restent l'outil de base de ces échanges, la CNCTR s'appuie également sur de nouveaux moyens de diffusion des informations.

Ainsi, les services sont régulièrement invités à présenter devant les membres de la CNCTR les thématiques, stratégies et difficultés rencontrées dans le cadre de leur action, que ce soit physiquement au sein des locaux de la commission ou récemment par le biais de visio-conférences sécurisées pour les interventions plus ponctuelles.

En retour, le partage de la doctrine de la CNCTR avec les services fait l'objet d'une attention toute particulière, avec la mise en place d'une diffusion systématique début 2024, par le biais de fiches d'alerte et d'une lettre annuelle.

Enfin, pierre angulaire du relationnel entre la commission et les services, les contrôles *a posteriori* réalisés *in situ* permettent d'aborder l'ensemble des sujets via l'action des chargés de mission « référents » du service concerné.

1.3. Les finalités invoquées à l'appui des demandes de mise en œuvre des techniques de renseignement : une répartition très similaire à celle observée en 2022

Reprenant la présentation adoptée dans chacun de ses rapports d'activité, la CNCTR mentionne, pour l'ensemble des demandes tendant à la mise en œuvre d'une technique de renseignement relevant de la surveillance domestique[18], la proportion de chacune des sept finalités énumérées par l'article L. 811-3 du code de la sécurité intérieure[19]. Cette répartition des techniques selon la finalité ne coïncide pas avec celle des personnes sous surveillance.

En effet, en fonction de la finalité poursuivie, la durée moyenne de surveillance des personnes ciblées varie fortement, de même que le nombre des techniques mises en œuvre. Concrètement, la surveillance d'une personne suivie au titre de la prévention du terrorisme mobilise en moyenne davantage de techniques que celle d'une personne surveillée au titre de la prévention de la délinquance et de la criminalité organisées[20].

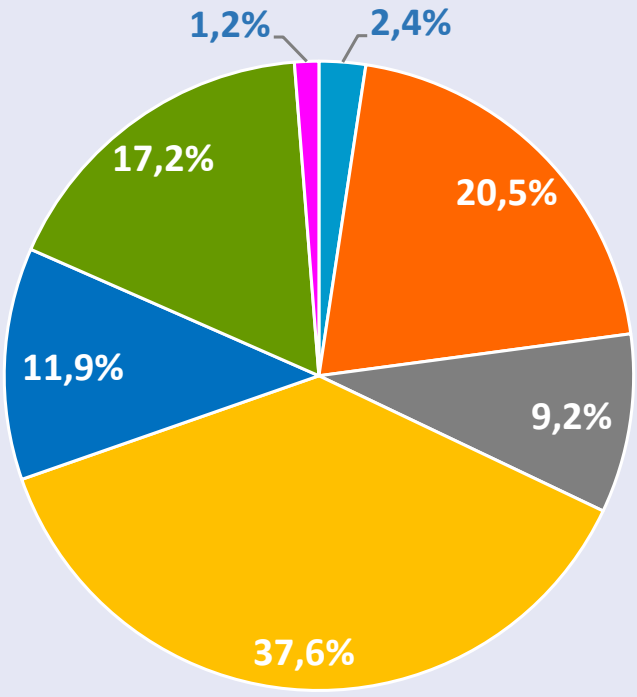
Les graphiques qui suivent présentent, pour le premier, la part prise par chacune des finalités prévues à l'article L. 811-3 du code de la sécurité intérieure dans le nombre total de demandes et, pour le second, l'évolution du nombre total de techniques sollicitées par finalité sur les quatre dernières années.

18. Il s'agit des techniques prévues aux chapitres I à III du titre V du livre VIII du code de la sécurité intérieure.

19. Il est à relever qu'outre les sept finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure, l'article L. 855-1 du même code donne un accès, au bénéfice du seul service national du renseignement pénitentiaire (SNRP), à un nombre limité de techniques pour une finalité qui lui est propre, à savoir la prévention des évasions et le maintien de la sécurité au sein des établissements pénitentiaires et des établissements de santé destinés à recevoir des personnes détenues. En 2023, cette finalité a été invoquée dans 0,1 % des demandes en œuvre de techniques de renseignement, cette proportion étant identique à celle enregistrée en 2021 et 2022. Au vu de la volumétrie très faible qu'elle représente, cette finalité, qui ne concerne par ailleurs qu'un seul service, ne figure pas dans les diagrammes établis.

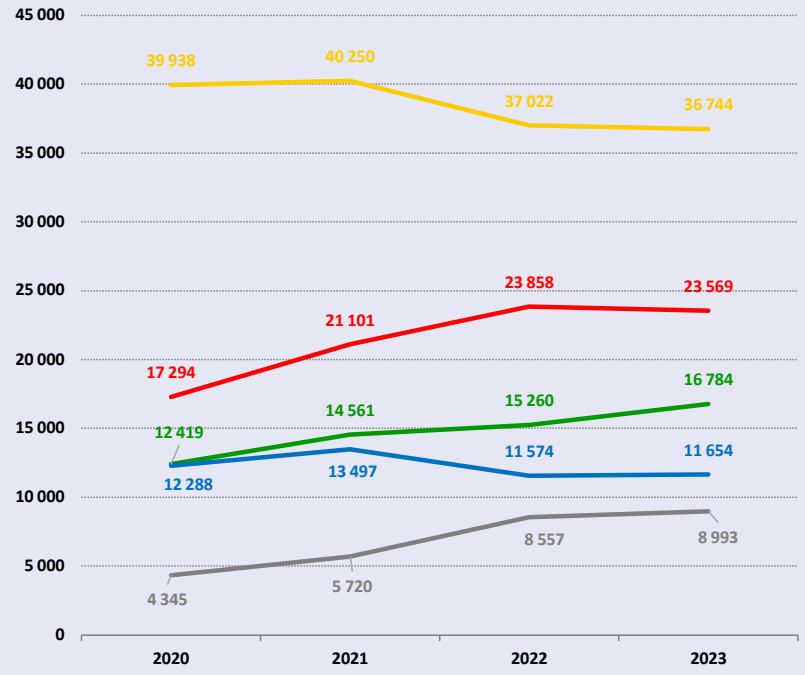
20. Voir point 1.2 ci-dessus, p. 30.

Les finalités fondant les demandes de techniques de renseignement en 2023



- 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

Evolution du nombre de demandes par finalité les motivant entre 2020 et 2023



La prévention du terrorisme

Les intérêts géostratégiques de la France (indépendance et défense nationales, intérêts majeurs de la politique étrangère et prévention de toute forme d'ingérence étrangère, lutte contre la prolifération des armes de destruction massive)

La prévention de la criminalité et de la délinquance organisées

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

Les intérêts économiques, industriels et scientifiques majeurs de la France

1.3.1. La prévention du terrorisme demeure la finalité la plus invoquée (en nombre de demandes)

Depuis 2015, le nombre de techniques de renseignement demandées au titre de la prévention du terrorisme demeure largement en tête même s'il a tendance à se stabiliser après les fortes augmentations en 2020 et 2021.

La part représentée par cette finalité parmi l'ensemble des techniques demandées diminue légèrement depuis 2020 et s'élève désormais à 37,6 %.

1.3.2. Une stabilisation du nombre des demandes présentées au titre des finalités liées aux intérêts géostratégiques de la France

Les demandes de techniques de renseignement fondées sur les trois finalités relevant des **intérêts géostratégiques de la France**[21] avaient enregistré, en 2020 et 2021 une forte augmentation. Elles demeurent en 2023 à un niveau comparable à celui constaté l'an passé à savoir un peu moins de 24 000 demandes (23 500 demandes contre 23 800 en 2022).

Cette relative stabilité à un niveau élevé résulte comme l'année dernière du contexte géopolitique international avec l'émergence, en différentes zones géographiques, de conflits armés aux répercussions mondiales, et des activités d'espionnage conduites par les services étrangers sur le territoire national qui demeurent à un niveau soutenu.

21. Cet agrégat regroupe les finalités prévues au 1°, 2° et 7° de l'article L. 811-3 du code de la sécurité intérieure à savoir : au 1°, l'indépendance nationale, l'intégrité du territoire et la défense nationale, au 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, et au 7°, la prévention de la prolifération des armes de destruction massive.

L'examen détaillé de ce groupe de finalités fait d'ailleurs apparaître que les demandes fondées sur la finalité mentionnée au 2° de l'article L. 811-3 du code de la sécurité intérieure, c'est à dire la prévention de toute forme d'ingérence étrangère, après avoir sensiblement cru en 2022, voient leur nombre augmenter encore.

1.3.3. Une légère hausse du nombre de demandes des techniques fondées sur la prévention de la criminalité et de la délinquance organisées en corrélation avec l'augmentation importante du nombre de personnes surveillées à ce titre

Comme en 2022, la prévention de la criminalité et de la délinquance organisées vient en troisième position du ratio des finalités invoquées par les services à l'appui de leurs demandes avec une part de 17 % des autorisations accordées. Le volume total des techniques sollicitées au titre de cette finalité ne cesse d'augmenter. Avec un accroissement de 10 % des demandes fondées sur cette finalité en un an, leur nombre s'élève cette année à 16 800 contre 15 200 en 2022 atteignant ainsi leur plus haute valeur au cours des cinq dernières années, traduction de l'activité intense des services en ce domaine.

1.3.4. Une stabilisation du nombre des demandes fondées sur la prévention des violences collectives malgré la baisse sensible du nombre de personnes surveillées à ce titre

Le nombre de demandes formulées au titre de la prévention des violences collectives demeure stable à 11 600. Toutefois, cette stabilisation du nombre de techniques sollicitées doit être mise en lien avec la baisse du nombre de personnes surveillées au titre de cette

finalité (voir point 1.1 ci-dessus) traduisant un meilleur ciblage des personnes d'intérêt par les services avec pour corollaire une surveillance plus intensive faisant appel à un nombre accru de techniques.

À cet égard, la CNCTR rappelle qu'elle se montre particulièrement vigilante sur la motivation des demandes présentées sur le fondement de la finalité mentionnée au c du 5° de l'article L. 811-3 du code de la sécurité intérieure, considérant que la prévention des violences collectives ne saurait s'interpréter comme un vecteur d'immixtion dans un milieu politique ou syndical ou encore de limitation du droit constitutionnel de manifester ses opinions, fussent-elles extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas allégué de manière suffisamment plausible.

Manifestation de cette vigilance accrue, la majorité des avis défavorables rendus par la commission en 2023, à l'instar des années précédentes, a concerné cette finalité. Pour autant, la CNCTR relève que le taux d'avis défavorables émis a tendance à s'infléchir alors que le nombre de demandes poursuivant ce motif légal demeure stable.

Comme elle l'indiquait dans son précédent rapport d'activité, la commission a mené un important travail de formalisation et de consolidation de sa doctrine, matérialisé sous la forme d'un recueil régulièrement mis jour et servant de référence dans le cadre du contrôle *a priori* des demandes. La diffusion de sa partie consacrée à la prévention des violences collectives au sein des services de renseignement a contribué au recul du nombre d'avis défavorables rendus en cette matière.

Enfin, le volume des demandes présentées sur le fondement de la **défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France** demeure relativement stable par rapport à 2022.

Les échanges économiques ayant désormais retrouvé leur niveau d'avant la crise sanitaire, la concurrence entre États, exacerbée et parfois agressive, ainsi que le risque élevé de captation d'informations stratégiques en matière économique, scientifique et technologique induisent une importante mobilisation des services en la matière.

Partie 2. Un renforcement sensible du contrôle *a posteriori* de l'usage des techniques de renseignement qui met à jour la récurrence d'anomalies de gravité variable

Le contrôle *a posteriori* qu'exerce la commission sur l'activité des services de renseignement revêt une triple dimension. 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. Enfin, il a également une dimension informative, pédagogique et relationnelle permettant de mieux comprendre les enjeux du service et la réalité du terrain en étant directement au contact des opérationnels mais aussi de dissiper les inévitables malentendus susceptibles de survenir.

Ce contrôle *a posteriori* constitue un enjeu crucial face à la crainte d'un écart qui irait croissant entre les moyens limités de la CNCTR, d'une part, et, d'autre part, l'utilisation de techniques de renseignement de plus en plus intrusives permettant la captation d'une masse de données sans commune mesure avec ce qu'elle était « au temps des écoutes », le recours à des systèmes de pré-traitement et de traitement de ces données de plus en plus sophistiqués et la complexité et la diversité de leurs conditions de stockage.

Cette réalité a conduit à faire du renforcement du contrôle *a posteriori* une priorité stratégique à ce stade de la vie de la commission, avec une meilleure sélectivité et un meilleur suivi de la correction des anomalies relevées.

2.1. Un contrôle *a posteriori* plus fréquent, mieux ciblé et plus efficient

2.1.1. | Un niveau de contrôle au sein des services sans précédent

Avec 136 contrôles sur pièces et sur place réalisés en 2023, tous services confondus, la commission a atteint, à moyens humains quasiment constants[22], le plus haut niveau de contrôles *a posteriori* depuis sa création en octobre 2015.

Cette évolution repose en particulier sur une augmentation très sensible du nombre de contrôles consacrés aux mesures de surveillance des communications électroniques internationales. Ainsi, 42 contrôles ont été menés en la matière s'agissant des six services de renseignement du premier cercle[23], à comparer avec la trentaine de contrôles réalisés en 2022 et la vingtaine de contrôles réalisés en 2021.

Cette très forte augmentation en deux ans s'explique par une évolution des modalités concrètes de contrôle vers moins de formalisme et plus de vérifications informatiques techniques, permettant à une délégation réduite de la commission d'accéder, au sein de chaque service, à un poste informatique dédié donnant accès aux données recueillies sur le fondement des dispositions des articles L. 854-1 et suivants du code de la sécurité intérieure. Lors de ces contrôles, les vérifications se concentrent sur

22. Si trois créations d'emplois supplémentaires ont été accordés à la commission au titre de l'exercice 2023 (voir le 7ème rapport d'activité 2022 de la CNCTR, p. 134) et qu'en conséquence deux nouveaux postes de chargés de mission ont pu être créés et un quatrième membre du collège mobilisé à temps plein notamment aux fins de permettre la réalisation d'un nombre plus important de contrôles sur place, le nouvel effectif théorique de 14 chargés de mission n'a en pratique été atteint que sur deux semaines sur l'ensemble de l'année 2023 en raison des départs intervenus et de difficultés de recrutement déjà signalées lors du précédent rapport annuel.

23. Les services spécialisés du renseignement, dits services du premier cercle, recouvrent la direction générale de la sécurité intérieure (DGSE), la direction générale de la sécurité intérieure (DGSI), la direction nationale du renseignement et des enquêtes douanières (DNRED), la direction du renseignement militaire (DRM), la direction du renseignement et de la sécurité de la défense (DRSD) et le service à compétence nationale dénommé « traitement du renseignement et de l'action contre les circuits financiers clandestins » (TRACFIN).

les données recueillies et les opérations d'exploitation effectuées permettant de limiter la mobilisation des agents du service concerné. Les demandes de justification des éventuelles anomalies découvertes sont adressées à l'issue du contrôle par un canal de communication sécurisée.

S'agissant des 94 contrôles consacrés aux techniques de surveillance dites domestiques, environ 80 ont été menés dans les locaux des administrations centrales, principalement ceux des services dits du premier cercle, et, comme en 2022, une quinzaine ont été effectués au sein des implantations territoriales des services ou du GIC, y compris en outre-mer[24].

2.1.2. De nouvelles possibilités de contrôle et de suivi à distance au service d'un contrôle mieux ciblé et plus efficient

Par ailleurs, ces chiffres ne rendent pas compte du développement des capacités de contrôle à distance de la commission au cours de l'année ainsi que de ses capacités de suivi et d'approfondissement.

En effet, dans la continuité de l'évaluation de ses méthodes de contrôle *a posteriori* menée en 2022[25], la commission s'est dotée de nouveaux outils de communication sécurisée et de contrôle à distance.

Elle dispose ainsi désormais dans ses locaux d'un outil de visioconférence sécurisée, de postes d'accès à distance aux communications électroniques internationales interceptées dites mixtes[26] et, dans une mesure encore très modeste, de moyens d'accès à certaines données captées par les dispositifs de sonorisation ou de vidéo, ou issues des recueils de données informatiques autorisés.

24. Voir point 1.2.3 ci-dessous.

25. Voir 7ème rapport d'activité 2022 de la CNCTR, p. 56 et suivantes.

26. Il s'agit des communications renvoyant à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national.

2.1.3. | Une meilleure présence sur les territoires

La CNCTR a réalisé au cours de l'année écoulée une quinzaine de visites dans les centres administrés par le GIC ainsi que dans les implantations des services en province (voir les encarts ci-dessous). Le maintien d'un volume élevé de ces déplacements dans les territoires, puisqu'il est de 50 % supérieur à celui que connaissait la commission avant la crise sanitaire de 2020-2021, permet de concrétiser sa volonté de mieux appréhender les problématiques et difficultés locales des services de renseignement mais également d'assurer un contrôle de l'ensemble de la chaine de demande et de mise en œuvre des techniques de recueil de renseignement.

Dans ce sens, ces déplacements ont également évolué dans leur objet. Alors qu'ils visaient principalement à permettre à la commission de rencontrer les responsables locaux des services de renseignement déconcentrés, afin d'échanger sur la réalité des enjeux du renseignement dans leurs zones respectives d'implantation et les difficultés rencontrées dans l'application du cadre légal, ils sont désormais associés à des actions de contrôle de données et de respect des procédures légales et réglementaires.

Ces déplacements s'opèrent à présent selon deux manières : soit dans le cadre d'un centre GIC, soit directement dans les locaux des services.

LES CONTRÔLES MENÉS DANS LES CENTRES TERRITORIAUX DU GIC

Ces contrôles consistent en une série d'entretiens, menés avec chaque service déconcentré, débutant généralement par un exposé de l'état général des menaces affectant le territoire concerné et leurs éventuelles particularités, et se poursuivant autour du bilan des techniques de renseignement mises en œuvre par les services concernés et des résultats obtenus.

Ces échanges permettent de revenir sur certains avis rendus par la commission et d'expliquer les éléments de doctrine afférents. Les services peuvent en outre saisir l'opportunité de ces rencontres pour porter à la connaissance de la commission des difficultés d'ordre technique ou juridique et évoquer leurs perspectives de travail.

Enfin, il arrive à la commission de mettre à profit ces déplacements pour rencontrer les grands acteurs locaux de la sécurité, préfets ou procureurs de la République, lorsque des sujets ou des particularités le justifient.

LES CONTRÔLES DANS LES IMPLANTATIONS LOCALES DES SERVICES

Mis en place au second semestre 2022, ces contrôles au sein même des implantations des services sur le territoire, sont apparus nécessaires à la commission, en complément des déplacements dans les centres territoriaux du GIC, à la fois pour parfaire sa connaissance de l'organisation et du fonctionnement des services et approfondir son contrôle.

En pratique, ces contrôles locaux peuvent être mis en œuvre dans un service précis sur décision du président ou du collège lorsqu'une irrégularité est suspectée, ou être réalisés dans plusieurs services en amont ou en aval d'un déplacement dans le centre GIC dont ils dépendent.

Lors de ces déplacements, outre des échanges pouvant se rapprocher de ceux tenus en centres GIC, il est procédé à un contrôle approfondi des procédures de mise en œuvre des techniques de renseignement, de stockage des matériels utilisés pour le recueil de données sensibles (comme les microphones, les balises, les *IMSI-catcher* ou les caméras dissimulables) et des données conservées localement. La bonne tenue des différents registres prévus par le code de la sécurité intérieure ou la réglementation découlant des articles 226-3 et R. 226 et suivants du code pénal[27] est également, le cas échéant, vérifiée.

27. L'article 226-3 du code pénal prévoit une peine de cinq ans d'emprisonnement et de 300 000 € d'amende notamment pour « *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'État, 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* ». Les articles R. 226-1 et suivants fixent les modalités selon lesquels ces dispositifs sont soumis à autorisation et instaurent une commission consultative, à laquelle un représentant de la CNCTR participe, dont le secrétariat est assuré par l'Agence nationale de la sécurité des systèmes d'information (voir l'article R. 226-2).

Ces déplacements sont également l'occasion de s'assurer de la bonne compréhension du cadre légal par les agents chargés de la mise en œuvre des techniques de renseignement. Ils permettent aussi de vérifier que les matériels utilisés pour le recueil de renseignement sont stockés de manière à limiter leur accès aux seuls agents habilités et qu'une traçabilité précise et vérifiée par un échelon hiérarchique adéquat garantit leur utilisation conformément à la loi. Enfin, des contrôles de données, réalisés directement sur les capteurs ou certains ordinateurs d'exploitation des données brutes, permettent de s'assurer que les services ne disposent pas de stocks d'informations qui dérogeraient aux règles imposées en matière de centralisation, de délais de conservation et de traçabilité.

Au total, à l'instar des années précédentes, la CNCTR dresse un bilan globalement satisfaisant des contrôles sur pièces et sur place qu'elle a diligentés en 2023. Les modalités d'échange avec les services dans le cadre de la préparation de ces contrôles sont d'une grande fluidité et les conditions dans lesquelles les délégations de la commission sont reçues dans les locaux des services n'appellent aucune observation.

Néanmoins, comme la commission a eu l'occasion de le souligner dans ses précédents rapports et malgré les mesures prises pour faire évoluer les modalités du contrôle *a posteriori*, les moyens humains et matériels dont elle dispose demeurent un facteur limitant alors que le nombre de techniques de renseignement mis en œuvre et la masse de données collectées ne cessent d'augmenter.

Par ailleurs, dans l'organisation concrète de ses contrôles sur place, la CNCTR est parfois confrontée à des difficultés logistiques et techniques (disponibilité des accès, complexité des réseaux, difficultés à localiser les données…) qui doivent conduire les services à poursuivre les démarches qu'ils ont entreprises en 2023 pour garantir la plénitude de ses accès aux données recueillies par la mise en œuvre de techniques de renseignement et aux résultats

de leur exploitation. Enfin, la commission considère que, lorsqu'il porte sur des modes de recueil de renseignements d'une particulière technicité, l'efficacité de son contrôle, tant *a priori* qu'*a posteriori*, suppose une connaissance accrue des possibilités offertes par les techniques concernées et des modalités de traitement des données recueillies. À cet égard, elle entend poursuivre le dialogue technique encourageant qui s'est établi avec les services au cours de l'année 2023 sans remettre en cause l'impératif de préservation de la confidentialité des modes opératoires qu'ils développent.

2.1.4. Un développement du contrôle qui résulte aussi de l'augmentation des réclamations des particuliers sans que cela conduise à une saisine plus importante de la formation spécialisée du Conseil d'État

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[28].

Le pouvoir de vérification que la loi a confié à la commission porte sur les seules techniques de renseignement prévues par le code de la sécurité intérieure, à savoir des techniques mises en œuvre par les services de renseignement dans l'exercice de leurs missions de police administrative. Cette compétence ne s'étend ni aux mesures de surveillance ordonnées par l'autorité judiciaire ni à celles, au demeurant 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

28. Cette procédure de réclamation préalable est prévue par les dispositions de l'article L.833-4 du code de la sécurité intérieure en ce qui concerne la surveillance nationale et par celles de l'article L. 854-9 du même code, en ce qui concerne la surveillance des communications électroniques internationales.

exceptions à l'application du droit des usagers de saisir l'administration par voie électronique, la CNCTR ne peut valablement être saisie que par lettre envoyée par voie postale. La réclamation doit être présentée par la personne concernée, 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 ont été communiqués à la commission.

La CNCTR instruit les réclamations qui lui sont adressées de la même manière et en utilisant les mêmes outils que lorsqu'elle effectue de sa propre initiative un contrôle a posteriori depuis ses locaux.

Des réclamations en hausse notable

Après une relative stabilité les années précédentes, le nombre de réclamations reçues par la CNCTR en 2023 a connu une augmentation de plus de 65 %.

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

Si les raisons d'une telle augmentation ne peuvent être totalement identifiées, la publication du nouveau site internet de la CNCTR, le 15 juin 2023, et plus particulièrement d'une page dédiée aux modalités de saisine de la commission (*https://www.cnctr.fr/saisir-la-commission*) a sans nul doute eu un impact sur le nombre de réclamations présentées.

Cet impact peut également être constaté sur la complétude des demandes de vérification reçues. En effet, le taux de demandes adressées à la CNCTR ayant pu être instruites sans avoir recours à une demande de

pièces complémentaires est passé de 18,37 % en 2022 à 34,38 % sur la période de 2023 postérieure à la publication du site internet.

S'agissant des réclamations multiples, trois personnes ont présenté plus d'une réclamation au cours de l'année 2023 et six réclamants ayant déjà saisi la CNCTR au cours des années antérieures ont souhaité que des vérifications soient à nouveau conduites à leur sujet.

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[29].

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. 8336 du code de la sécurité intérieure.

LE DISPOSITIF PROPRE AUX « LANCEURS D'ALERTE »

Pour garantir qu'il soit mis fin aux éventuelles violations manifestes du cadre juridique applicable aux techniques de renseignement, l'article L. 861-3 du code de la sécurité intérieure prévoit que les agents des services de renseignement ayant connaissance, dans l'exercice de leurs fonctions, d'une telle violation, peuvent porter ces faits à la connaissance de la seule CNCTR. Il appartient alors à la commission, au vu des éléments qui lui ont été transmis, de faire usage, le cas échéant, des pouvoirs de contrôle que lui attribue la loi.

Ces dispositions n'ont pas reçu application depuis l'entrée en vigueur du cadre légal en 2015.

29. 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.

Un recours au juge qui demeure rare

La procédure contentieuse spéciale prévue aux articles L. 773-1 et suivants du code de justice administrative permet 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 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 code de la sécurité intérieure, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR.

S'agissant des mesures de surveillance des communications électroniques internationales, seul 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 la France. Ces personnes peuvent saisir elles-mêmes le Conseil d'État après réclamation préalable auprès de la commission. Ces hypothèses n'ont pas trouvé à s'appliquer en 2023.

Cinq nouvelles requêtes ont été enregistrées devant le Conseil d'État sur le fondement de l'article L. 8411 du code de la sécurité intérieure en 2023 et quatre décisions ont été rendues.

Au 31 décembre 2023, quatre affaires enregistrées en 2023 demeuraient en instance.

La CNCTR est informée de toute requête introduite sur le fondement de l'article L. 841-1 du code de la sécurité intérieure 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.

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. 8338 code de la sécurité intérieure. 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) aux avis ou aux recommandations de la commission[30].

Des modalités de contrôle perfectibles en matière de surveillance internationale

En application des dispositions de l'alinéa 4 de l'article L. 854-9 du code de la sécurité intérieure, la CNCTR peut être saisie par toute personne qui souhaite vérifier qu'aucune mesure de surveillance internationale ou de vérification ponctuelle[31] n'est irrégulièrement mise en œuvre à son égard. La commission s'assure alors que les mesures de surveillance des communications électroniques internationales éventuellement mises en œuvre respectent le cadre légal et réglementaire applicable ainsi que les décisions et autorisations du Premier ministre.

30. 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. 8211 du code de la sécurité intérieure 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.

31. 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. A 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 notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer la mise en œuvre de mesures de surveillance ou de vérification ponctuelle.

En 2023, une seule réclamation a porté sur la vérification de la régularité de la mise en œuvre de mesures de surveillance internationale.

Si la commission dispose d'outils lui permettant d'exercer le contrôle qui lui incombe depuis ses locaux pour un certain nombre des techniques mises en œuvre en surveillance intérieure, il n'en est pas de même s'agissant de la surveillance internationale.

L'absence d'accès à distance aux applications informatiques sécurisées alourdit considérablement les opérations de contrôle en la matière, imposant ainsi à une délégation de la commission de se rendre dans chacun des services spécialisés de renseignement afin de procéder aux opérations de contrôle nécessaires, qui peuvent être longues et complexes.

Au vu de l'évolution du nombre de réclamations dont elle est saisie, la CNCTR considère qu'une amélioration des conditions de son contrôle en matière de surveillance internationale est nécessaire. Si cette amélioration peut prendre, dans un premier temps, la forme d'un accès aux communications dites mixtes[32] depuis les locaux de la commission et d'une mise à disposition (intervenues début 2024) d'une salle dédiée à la commission avec un accès aux données de chacun des services spécialisés de renseignement dans un laps de temps resserré et sans contraintes organisationnelles préalables, la CNCTR estime indispensable à moyen terme d'aller plus loin en organisant un accès depuis ses propres locaux à l'ensemble des systèmes d'information permettant de contrôler les dispositifs de traçabilité, les renseignements collectés, les transcriptions, extractions, transmissions et relevés visés à l'article L. 854-9 du code de la sécurité intérieure comme cela devrait être à terme le cas en matière de recueil des données informatiques (voir point 3.1 ci-dessous).

32. C'est à dire renvoyant pour partie à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national.

2.2. Les efforts réalisés par les services ne suffisent pas encore à prévenir la récurrence de certains manquements

À l'occasion de ses contrôles *a posteriori* réalisés en 2023, la CNCTR a relevé, comme les années précédentes, un certain nombre d'irrégularités, à chaque étape du cycle de vie de la technique de renseignement : de la mise en œuvre d'une technique à l'exploitation des données recueillies tant en matière de surveillance intérieure que de surveillance internationale.

Si les irrégularités relatives aux modalités de mise en œuvre des techniques (périmètre, champ d'application…) sont de plus en plus rares, elles sont aussi les plus sensibles en termes d'atteinte aux libertés individuelles dans la mesure où elles ont conduit au recueil de données qui n'auraient pas dû être collectées (2.2.1). En matière d'exploitation du produit des techniques, les anomalies relevées ne présentent pas, pour la plupart, un caractère majeur ; elles posent néanmoins question au regard de leur récurrence ou de leur persistance d'une année sur l'autre et ce malgré les mesures prises par les services pour améliorer les pratiques (2.2.2).

2.2.1. Les anomalies constatées dans la phase de mise en œuvre des techniques de renseignement : peu nombreuses mais à fort enjeu en termes de libertés publiques

Les anomalies liées à la diversité des possibilités offertes par les techniques

À l'instar des années précédentes, la commission a relevé un certain nombre de cas où un service, pour installer une technique, s'est introduit dans un lieu privé sans disposer de l'autorisation nécessaire.

Il arrive en effet qu'un service n'anticipe pas la nécessité de devoir s'introduire dans un lieu privé[33], le cas échéant à usage d'habitation, ou omette cette éventualité dans la motivation de sa demande. Au stade de l'instruction de celle-ci, l'absence d'une telle information peut fausser le contrôle de proportionnalité auquel se livre la commission. Après autorisation, le contrôle mené *a posteriori* peut révéler une introduction non prévue dans un lieu privé à usage d'habitation alors que cette mesure n'est ouverte qu'à un nombre limité de services et pour un nombre limité de finalités.

Ainsi, même si ce type d'irrégularité est désormais rare, elle constitue une atteinte caractérisée à la vie privée et peut engager la responsabilité pénale des agents chargés de l'opération.

Les imprécisions ou les omissions dans la demande peuvent également vicier l'examen des demandes tendant au recueil de données informatiques. En effet, cette technique, traitée de façon très concise par le législateur, recouvre en pratique des modes opératoires très différents dont le caractère intrusif peut fortement varier. Or, les précisions relatives aux modalités du recueil envisagé par le service, au nombre et au type de dispositifs déployés ou encore aux espaces et supports de stockage utilisés pour la mise en œuvre de la technique ont une incidence directe sur l'appréciation de la proportionnalité de la mesure. Les services sont dès lors régulièrement invités par la commission à détailler davantage leur demande et à expliciter le contexte opérationnel ainsi que les résultats concrets recherchés par la mise en œuvre de cette technique.

La commission peut être amenée à rendre des avis restrictifs conduisant à ce que l'autorisation accordée ne porte que sur certains modes opératoires ou encore sur certains supports. Or, dans de rares cas il est vrai, les contrôles menés *a posteriori* ont

33. L'introduction dans un véhicule ou un lieu privé (ILP) est prévue par les dispositions de l'article L. 853-3 du code de la sécurité intérieure. Si le lieu privé concerné constitue un lieu d'habitation, l'avis de la commission relève de l'une de ses formations collégiales.

pu révéler une mise en œuvre de la technique qui ne correspond pas à la description apparaissant dans la demande, comporte des aspects non prévus ou encore ne respecte pas certaines restrictions fixées par la commission. Ces irrégularités ont pour effet de conduire à recueillir des données qui n'auraient pas dû être collectées.

Les anomalies tenant au dépassement de la durée d'autorisation ou de la durée pertinente de captation

De manière moins fréquente que l'année précédente, la CNCTR a constaté des dépassements de la durée d'autorisation de mise en œuvre permise par le cadre légal. Ces dépassements ont en pratique pu aller jusqu'à une dizaine de jours.

Par ailleurs, elle a relevé des irrégularités tenant à une mise en œuvre effective de la technique au-delà de l'objet de la surveillance. Il peut s'agir d'hypothèses où le service a continué à opérer une technique alors que la personne ciblée n'était pas ou plus présente dans le lieu prévu ou a procédé à une mise en œuvre trop étendue de la technique par rapport à un événement limité dans le temps. Ces pratiques irrégulières résultent le plus souvent d'une difficulté technique dans le paramétrage du dispositif de surveillance ou de contraintes opérationnelles ne permettant pas toujours au service d'intervenir pour limiter la mise en œuvre de la technique au strict nécessaire.

Les anomalies tenant à la traçabilité des actions effectuées par les services de renseignement

En dépit des efforts constatés cette année, un certain nombre d'irrégularités sont toujours relevées en matière de respect des exigences de traçabilité[34]. Ainsi, les contrôles *a posteriori* menés par

34. Aux termes de l'article L. 822-1 du code de la sécurité intérieure, 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 « fiche de traçabilité », est tenu à la disposition de la CNCTR qui peut y accéder de manière permanente, complète et directe quel que soit son degré d'achèvement.

la commission ont pu révéler l'absence de fiches de traçabilité, leur établissement trop tardif ou encore leur caractère incomplet. Le nombre de ces anomalies varie selon le type de technique mise en œuvre et les services en cause. En effet, les différences d'organisation au sein des services ou encore les différents modes de recueil des données peuvent conduire à des délais d'établissement des fiches de traçabilité variables et avoir une incidence sur la qualité du suivi relaté.

Ainsi, même si les exigences en la matière tendent à être de plus en plus respectées par les services - la commission les rappelant régulièrement en amont comme en aval de ses contrôles, des irrégularités en matière de traçabilité sont encore constatées notamment lors des changements de dispositifs (en cas de panne, de retrait ou d'échange de ces derniers) ou encore de changement de situation opérationnelle. Elles peuvent également prendre la forme d'erreurs ou d'omissions dans les dates relevées, ou d'insuffisance dans le descriptif des dispositifs employés ou encore des lieux de déploiement.

L'enjeu est important pour la commission dans la mesure où seul le correct établissement de ces éléments de traçabilité permet à la fois de préparer efficacement les contrôles effectués dans les services et d'améliorer l'instruction des éventuelles demandes de renouvellement des techniques concernées.

La commission encourage donc les services à faire toujours preuve d'attention et de rigueur dans l'établissement de la traçabilité des éléments propres à chaque technique et au contexte opérationnel rencontré, y compris lorsqu'une technique n'a pas pu être mises en œuvre, notamment en indiquant de façon exhaustive et précise les actions réalisées sur les sélecteurs techniques ajoutés, modifiés ou supprimés.

2.2.2. Les anomalies constatées au stade de l'exploitation des données : moins problématiques en termes d'atteinte aux libertés publiques, leur récurrence et leur persistance au fil des ans posent néanmoins question

Plus importantes quantitativement, ces anomalies constituent des atteintes d'une gravité moindre que celles relevées au stade de la mise en œuvre des techniques dans la mesure où elles portent sur des données dont les services disposent légitimement puisqu'elles ont régulièrement été collectées. Néanmoins, leur caractère récurrent et persistant conduit à appeler les services à poursuivre leurs efforts en matière de formation et de contrôle interne.

Les irrégularités relevées en matière de surveillance domestique

Des dépassements de la durée légale de conservation des données brutes obtenues.

Le code de la sécurité intérieure prévoit en son article L. 822-2, que les renseignements collectés, y compris lorsqu'ils n'ont pas été intégralement exploités, doivent être détruits avant l'expiration d'un certain délai, dont la durée varie en fonction de la nature des données et de l'atteinte portée à la vie privée.

Dans deux cas en 2023, les données indûment conservées provenaient d'une technique de captation de paroles prononcées à titre privé[35].

Dans le premier cas, il est apparu que ces données étaient conservées sur un serveur non soumis à un script d'effacement automatique et qu'un manque de vigilance, admis par le service concerné, était à l'origine de cette conservation au-delà du délai légal. Sur les recommandations de la commission, les données ont été rapidement détruites et il en a été justifié par production d'un procès-verbal.

35. Voir l'article L. 853-1 du code de la sécurité intérieure.

Dans le second cas, bien que le serveur sur lequel les données étaient hébergées disposât d'un script automatisant l'effacement, le délai de destruction n'a pas été respecté parce que le point de départ du délai de conservation était erroné. Le service concerné par cette anomalie, qui avait déjà été confronté à une problématique similaire l'année dernière et y avait remédié sur un autre de ses systèmes d'information, a étendu les correctifs au serveur concerné et a procédé, conformément à la demande de la CNCTR, à la destruction des données indûment conservées.

En 2022, 19 anomalies de ce type avaient été observées. Il s'agissait de cas où des données avaient été recueillies par la technique de recueil de données informatiques[36].

La CNCTR souligne à cet égard que ces recueils de données, parmi les plus attentatoires à la vie privée, échappent encore largement au dispositif de centralisation organisé par le GIC même si des avancées significatives sont intervenues en la matière en 2023 (voir partie 3 du présent rapport). Il en résulte que le respect des règles de conservation et d'exploitation des données collectées repose sur la fiabilité et la rigueur des procédures internes mises en place par les services.

La commission appelle donc de ses voeux la poursuite des efforts menés par le GIC en 2023 pour mettre en place une solution de centralisation partielle et limitée à certains services, notamment par le développement de réseaux informatiques sécurisés permettant l'acheminement d'un volume conséquent de données. S'agissant des « grands » services recourant à ce jour à des dispositifs de centralisation propres, la CNCTR se félicite de la perspective d'une centralisation au GIC à moyenne échéance dans le respect de leurs capacités opérationnelles (voir partie 3 du présent rapport).

Cependant, dans l'attente de ces développements, la CNCTR appelle l'ensemble des services à la plus grande vigilance quant au recours, en hausse depuis quatre années, à cette technique.

36. Voir le rapport d'activité 2022 de la CNCTR, p. 42.

Des transcriptions abusives

Comme en 2023, l'irrégularité la plus fréquemment relevée au cours des contrôles *a posteriori* consiste en des retranscriptions d'éléments ne présentant aucun lien avec la ou les finalités ayant justifié le recueil de renseignements, ni même, dans des cas plus rares, avec la personne surveillée.

En ce domaine, l'enjeu de protection de la vie privée est d'autant plus prégnant que, contrairement aux données dites « brutes » obéissant à des délais de conservation contraints[37], les transcriptions et extractions, en ce qu'elles constituent des données « pertinentes », peuvent être conservées tant qu'elles demeurent indispensables à la poursuite d'une des finalités légales[38].

L'appréciation de l'opportunité de la conservation de ces données peut parfois s'avérer très délicate alors que l'évaluation de la pertinence de la stratégie d'enquête adoptée par les services n'entre pas dans les prérogatives de la commission. En revanche, il appartient à celle-ci d'apprécier l'existence d'un lien entre les informations conservées et les finalités légales. Pour ce faire, la CNCTR procède à un contrôle plus ciblé mais aussi plus approfondi[39] que celui mené de façon systématique par le bureau contrôle du GIC sur les techniques faisant l'objet d'une centralisation [40].

Ce contrôle est réalisé aussi bien pour l'instruction des demandes de renouvellement d'une technique que dans la perspective des contrôles sur pièces et sur place. Ces vérifications peuvent être

37. Voir l'article L. 822-2 du code de la sécurité intérieure

38. Voir le III de l'article L. 822-3 du code de la sécurité intérieure

39. Ce contrôle est réalisé grâce aux applications informatiques sécurisées mises à la disposition de la commission par le GIC lesquelles lui permettent d'accéder, à tout moment, directement depuis ses locaux, à l'ensemble des transcriptions réalisées à partir des interceptions de sécurité ainsi qu'à celles issues des techniques de captations de paroles et d'images qui sont centralisées.

40. Avant sa mise à disposition aux agents du service concerné, tout projet de transcription ou d'extraction est soumis à la validation du bureau contrôle du GIC qui s'assure que les informations qui y figurent se rapportent bien à la cible désignée dans l'autorisation de technique de renseignement et que la traçabilité de cette exploitation est correctement remplie. De plus, une vérification est opérée sur l'adéquation entre le contenu même de la « production » et l'objet de la surveillance. Lorsque le GIC identifie une difficulté, il engage un dialogue avec le service qui peut aboutir à la validation et à la diffusion de la « production » ou, à l'inverse, à la suppression des contenus litigieux.

menées spontanément, à l'initiative d'un chargé de mission ou du pôle du contrôle *a posteriori*, ou de manière programmée, certains avis conditionnant en effet le renouvellement d'une autorisation au suivi des résultats de l'exploitation de la technique considérée.

Lorsqu'apparaît une interrogation quant à la pertinence des éléments figurant dans une ou plusieurs transcriptions, un échange s'instaure avec le service[41] afin de déterminer si la ou les productions doivent être détruites ou peuvent au contraire être conservées.

En 2023, l'ensemble des productions pour lesquelles la CNCTR a confirmé sa demande de destruction à l'issue du dialogue avec le service ont été détruites dans des délais satisfaisants.

Dans le cadre de ce contrôle renforcé, la CNCTR prête une attention particulière aux transcriptions et extractions issues des techniques de renseignement autorisées à l'égard des personnes exerçant une profession ou un mandat dits « protégés »[42]. En effet, les dispositions de l'article L. 821-7 du code de la sécurité intérieure font obstacle à ce que ces personnes fassent l'objet d'une mesure de surveillance à raison de leur profession ou de leur mandat[43].

Parmi les anomalies constatées en 2023, deux ont été relevées dans le cadre de la surveillance de ces professions protégées. Ainsi, la commission a constaté que les services avaient retranscrit des éléments les concernant qui étaient directement liés à leur profession.

Ces irrégularités ont donné lieu à des demandes de destruction des données ainsi capitalisées auxquelles les services concernés ont rapidement donné suite.

41. Voir le c) de la présente partie ci-dessous.

42. Il s'agit des parlementaires, des avocats, des magistrats et des journalistes.

43. L'article L. 854-3 du code de la sécurité intérieure prévoit une protection similaire dans le cadre de la surveillance des communications électroniques internationales de ces personnes lorsque ces dernières exercent leur profession ou mandat sur le territoire national. Voir sur ce point l'étude figurant 7ème rapport d'activité 2022 de la CNCTR, p.93 et suivantes

Dans un cas, un contrôle sur pièces et sur place a révélé qu'un service avait conservé des données qui, bien que pertinentes au regard de la finalité poursuivie au moment de leur recueil, étaient relatives à des investigations qui avaient d'ores et déjà permis d'écarter finalement tout lien avec cette finalité. En pratique, l'anomalie relevée ne résultait pas d'une volonté délibérée de contourner le cadre légal mais d'une mauvaise compréhension de sa portée dans une telle configuration. Ce cadre légal applicable a été rappelé et précisé par la commission et les données litigieuses ont été détruites par le service concerné.

Des difficultés persistantes en matière d'établissement des bulletins de renseignement relatant les actions d'exploitation des données recueillies

L'article L. 822-4 du code de la sécurité intérieure dispose que les transcriptions et extractions font l'objet de relevés tenus à la disposition de la commission, la loi lui garantissant par ailleurs un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions.

À plusieurs reprises en 2023, la commission s'est aperçue que des transcriptions ou extractions n'avaient donné lieu à aucun établissement de bulletin de renseignement ou n'avaient pas été centralisées par le service si bien qu'elles s'avéraient inaccessibles à la commission et, donc, échappaient à son contrôle alors que ces bulletins sont destinés à capitaliser les informations pertinentes qui auront vocation à être conservées.

Ces irrégularités révèlent que, malgré le développement de systèmes d'information dédiés à l'exploitation des données issues de la mise en œuvre des techniques de renseignement, nombreux sont encore les agents qui persistent à travailler sur des fichiers propres non centralisés, à partir de leur propre poste de travail, sans aucune traçabilité.

Déjà dressé en 2022, ce constat, préoccupant en ce qu'il met en lumière un risque de dispersion peu voire non contrôlée des données collectées, avait conduit la commission à engager un dialogue avec les entités chargées du contrôle interne au sein des services concernés. Si des progrès avaient alors été enregistrés tant en ce qui concerne les délais d'établissement des bulletins de renseignement que leur caractère complet, force est de constater qu'ils n'ont pas suffisamment été poursuivis en fin d'année 2023 et que la difficulté est récurrente dans certains services.

La CNCTR en appelle donc à la constante vigilance et au renouvellement des efforts des services de contrôle interne afin de résoudre durablement ces difficultés.

Les irrégularités constatées en matière de surveillance des communications électroniques internationales

Comme en matière de surveillance intérieure, la CNCTR diligente régulièrement des contrôles des données issues de la surveillance des communications électroniques internationales, qu'il s'agisse des conditions de leur recueil, de leur conservation ou de leur exploitation.

Alors qu'elle ne disposait jusqu'en octobre 2023 d'aucun accès aux données ou aux traces de recherches effectuées par les agents des services, la CNCTR est désormais équipée de deux postes informatiques lui permettant d'accéder aux transcriptions des communications dites mixtes (c'est-à-dire renvoyant pour partie à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national).

Résultat d'un travail de concertation mené entre la CNCTR, le GIC et la direction générale de la sécurité extérieure, la mise à disposition de ces équipements constitue un progrès marquant dans le contrôle de la surveillance internationale permettant à la commission d'accéder désormais directement aux renseignements recueillis.

Au cours de l'année 2023, des irrégularités de même nature que celles enregistrées en 2022 ont été relevées au cours des différents contrôles réalisés par la CNCTR.

Des exploitations de données réalisées en méconnaissance des dispositions légales

En vertu de l'article L. 854-1 du code de la sécurité intérieure, les mesures de surveillance des communications électroniques internationales obéissent au principe général selon lequel la surveillance internationale ne permet pas, sauf exceptions expressément prévues par la loi, d'intercepter des communications nationales.

À plusieurs reprises en 2023, la CNCTR a relevé que des services avaient procédé, en dehors des exceptions légales, à des interrogations sur des identifiants techniques rattachables au territoire national qui étaient en communication avec une personne se trouvant sur le territoire national.

Par ailleurs, alors que la transcription d'une communication interceptée dans le cadre de la surveillance internationale suppose, en vertu du principe rappelé ci-dessus, qu'au moins une partie de cette communication présente un critère d'extranéité, la commission a, dans plusieurs services, constaté que des transcriptions faisaient état de communications intervenant entre deux personnes situées sur le territoire national au moment de l'interception.

La CNCTR a également découvert à trois reprises que l'exploitation des communications excédait le périmètre des autorisations délivrées par le Premier ministre. Du point de vue de la commission, ces irrégularités, quoique quantitativement limitées, constituent des manquements très sérieux.

Il a enfin été constaté qu'un agent avait, sans autorisation, effectué des recherches dans un espace de stockage de données bénéficiant

d'une protection spécifique sans qu'il ait pu être déterminé, d'une part, si les requêtes effectuées portaient sur des données de connexion[44] ou du contenu, d'autre part, si elles avaient permis à l'exploitant d'accéder effectivement à ces données.

Des consultations ou des exploitations ne se rattachant pas à l'autorisation pertinente

Tout comme l'an passé, les anomalies les plus fréquemment relevées mais également les plus bénignes consistent en la consultation ou l'exploitation de données que l'agent ne rattache pas à l'autorisation pertinente.

L'exploitation des données issues de la surveillance des communications électroniques internationales est réalisée par des agents spécialisés, à partir d'applications informatiques spécifiques dont les droits et les conditions matérielles d'accès sont strictement limités et contrôlés. Cette exploitation consiste, pour les agents concernés, en l'interrogation des bases abritant les données par la formulation d'une « requête » fondée sur l'autorisation d'exploitation dont bénéficie le service.

Aussi la CNCTR vérifie-t-elle que les éléments recherchés sont effectivement en lien avec l'objet de la mesure de surveillance autorisée, qu'il s'agisse des cibles suivies comme des finalités légales poursuivies.

Cette année encore, la commission a régulièrement constaté que des consultations voire des exploitations de données avaient été informatiquement rattachées à des autorisations non pertinentes.

Il ressort des explications apportées par les services que des négligences de la part des agents exploitants ou des erreurs de manipulation de l'outil informatique[45] sont à l'origine de ces anomalies.

44. Dans une telle hypothèse, cette requête pourrait relever du régime des vérifications ponctuelles (voir ci-dessous) et ne pas constituer une irrégularité.

45. L'outil informatique assiste en effet l'utilisateur en lui proposant automatiquement, à chaque nouvelle requête, l'autorisation d'exploitation invoquée pour la requête précédente.

Malgré les actions de formation des agents procédant à l'exploitation de la surveillance internationale et bien qu'en recul, la fréquence de ces anomalies demeure à un niveau qui doit, du point de vue de la commission, inciter les services à la poursuite de ces actions de formation lesquelles, conjuguées aux rappels réguliers effectués par les directions et bureaux juridiques concernés, doivent aboutir à endiguer durablement ces irrégularités.

Des irrégularités en matière de vérifications ponctuelles

D'autres irrégularités ont par ailleurs été constatées dans la pratique des « vérifications ponctuelles ». Prévues par le IV de l'article L. 854-2 du code de la sécurité intérieure, ces vérifications ponctuelles permettent de déroger au principe interdisant d'utiliser les mesures de surveillance internationale pour intercepter des communications nationales. Elles permettent de détecter, au sein des données de connexion, une menace aux intérêts fondamentaux de la Nation liée aux relations entre des numéros d'abonnement ou des identifiants techniques rattachables au territoire national et des zones géographiques, des organisations ou des personnes faisant l'objet d'une surveillance.

Dans deux hypothèses, ces dispositions légales prévoient en outre que ces vérifications peuvent être opérées sur des données dites « de contenu », par essence plus attentatoires à la vie privée. Il s'agit, d'une part, de détecter de manière urgente une menace terroriste. Les numéros et identifiants doivent alors être immédiatement communiqués au Premier ministre et à la CNCTR pour les besoins du contrôle. Il s'agit, d'autre part, de permettre la détection d'éléments de cyberattaque susceptibles de porter atteinte à l'indépendance nationale, l'intégrité du territoire ou la défense nationale.

Les recherches effectuées dans ce cadre ne peuvent excéder une certaine durée. Or, la commission a cette année encore constaté que cette condition n'avait pas été respectée et que des vérifications ponctuelles sur des communications avaient été effectuées en dehors des prescriptions légales.

2.2.3. Les suites données aux irrégularités et anomalies détectées : des services disposés à les corriger ; des vérifications ultérieures parfois nécessaires et des progrès à accomplir pour prévenir leur renouvellement

Lorsqu'un contrôle *a posteriori* conduit à la découverte d'une anomalie ou d'une irrégularité, la CNCTR met en œuvre une procédure instituée depuis plusieurs années et produisant à son sens des résultats satisfaisants.

Ainsi, le service concerné est systématiquement informé afin qu'un échange contradictoire soit initié. La discussion s'engage tout d'abord de manière informelle au cours du contrôle et se poursuit par une notification écrite adressée par voie sécurisée au service l'invitant à faire valoir ses observations.

Tout comme en 2022, l'intégralité des constats et analyses dressés par la commission cette année a été partagée par les services qui ont veillé à y mettre un terme dans de courts délais, sans que la commission ait à faire usage du pouvoir de recommandation formelle que lui confère l'article L. 833-6 du code de la sécurité intérieure.

La CNCTR s'est ainsi assurée que toutes les données brutes illégalement conservées avaient été détruites et n'avaient donné lieu à aucune exploitation.

S'agissant des transcriptions et extractions, le dialogue engagé avec les services a systématiquement abouti à une solution conjointement admise. Ainsi, selon les cas, ces échanges ont conduit à la justification de leur conservation au regard des éléments apportés par le service ou, au contraire, à la confirmation de la demande de destruction. Dans cette seconde hypothèse, la commission sollicite la communication des procès-verbaux de destruction et peut, le cas échéant, procéder à des vérifications au sein des systèmes d'information dans lesquels sont conservées les données.

Si les destructions demandées interviennent dans des délais jugés satisfaisants par la commission, ses vérifications ont plusieurs fois mis en lumière que les procès-verbaux *ad hoc* qui lui étaient adressés étaient erronés, soit que ceux-ci ne portaient pas mention de l'intégralité des données ou des transcriptions et extractions détruites, soit qu'elles étaient incorrectement ou incomplètement référencées.

La CNCTR attache beaucoup d'importance à la qualité de la rédaction de ces procès-verbaux et incite les services à y apporter le plus grand soin. En effet, ces actes constituent un engagement formel par lequel le service atteste de la réalité de la destruction des données brutes indûment conservées ou des transcriptions et extractions irrégulières ou devenues sans objet. La sincérité et l'exactitude des indications portées dans ces procès-verbaux apparaissent donc primordiales.

Au-delà du seul constat des anomalies et irrégularités, la commission s'attache à identifier précisément la ou les étapes des processus internes au cours desquels sont survenues les irrégularités afin d'envisager, en concertation avec le service concerné, les ajustements et correctifs à apporter afin de prévenir toute réitération.

Sa mission ne se borne en effet pas à la correction des irrégularités passées. Elle consiste également à s'assurer, pour l'avenir, de l'absence de renouvellement. Pour y parvenir, elle accompagne et, dans certains cas, guide la mise en œuvre de bonnes pratiques au sein des services pour assurer le plein respect du cadre légal.

Les irrégularités et anomalies décelées en 2023 n'ont pas révélé de volonté délibérée de dissimulation ou de contournement du cadre légal.

Elles témoignent toutefois de difficultés persistantes d'appropriation des bonnes pratiques par certains agents des services de renseignement. Les services juridiques ont depuis plusieurs années entrepris des actions de diffusion et d'explication du cadre d'emploi des techniques

de renseignement à l'attention de chaque acteur intervenant dans leur cycle de vie. Si la commission invite à la poursuite de ces démarches, des progrès demeurent encore à accomplir. En particulier, les procédures internes destinées à centraliser l'exploitation des techniques dans des systèmes d'information accessibles à la commission ne sont toujours pas correctement appliquées.

En outre, la répétition d'une année sur l'autre d'anomalies, même de faible gravité, témoigne de la persistance d'erreurs élémentaires résultant de la non-intégration, dans les méthodes de travail quotidiennes, des rappels et recommandations de la commission qui ne sont suivis d'effets qu'au coup par coup.

Plus de huit ans après l'entrée en vigueur de la loi du 24 juillet 2015, la commission constate que de mêmes anomalies et irrégularités persistent durablement d'une année sur l'autre. Cette situation montre que les mesures préventives déployées par les services sont insuffisamment efficaces. Ce constat est préoccupant dans un contexte d'augmentation substantielle du volume des données recueillies au moyen de techniques de renseignement particulièrement attentatoires à la vie privée et de complexification des systèmes assurant leur traitement.

Aussi, la CNCTR estime-t-elle que, pour garantir un niveau d'efficacité et de fiabilité acceptable de son contrôle *a posteriori* et face aux enjeux posés notamment par l'essor du recueil de données informatiques, les modalités d'exercice de ce contrôle doivent nécessairement évoluer vers un accès à distance (voir partie 3 du présent rapport).

Partie 3. Les sujets de vigilance et les perspectives pour les années à venir

3.1. Le recueil de données informatiques : poursuivre l'amélioration du contrôle[46]

3.1.1. L'enjeu particulier de la technique de recueil de données informatiques dans la mission de contrôle *a posteriori* de la commission

La commission souhaite insister, dans ce rapport 2023, sur l'enjeu que constitue le contrôle *a posteriori* des données informatiques recueillies suite à la mise en œuvre de techniques de renseignement autorisées. Elle n'a pour autant pas exclu de ses axes d'effort le contrôle *a priori* des demandes tendant à cette mise en œuvre. En tant que de besoin, elle a ainsi décidé d'assortir ses avis favorables de restrictions destinées à encadrer les capacités de collecte de données afin de mieux assurer le respect du principe de proportionnalité et de protéger les libertés individuelles.

De tels avis restrictifs risqueraient d'être dépourvus de portée si la commission ne disposait pas, en aval, des connaissances techniques et des capacités de contrôle, sur place ou à distance, suffisantes pour lui permettre d'en vérifier la correcte application. À cet égard, l'année 2023 a été riche en développements.

46. La technique de recueil des données informatiques est mentionnée à l'article L. 853-2 du code de la sécurité intérieure qui dispose notamment que : « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre, et permettant d'accéder à ces mêmes données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques.* »

Ainsi que l'avait souligné la commission, ces progrès étaient nécessaires pour assurer un contrôle efficace d'une technique présentant de fortes particularités. Celles-ci ne se limitent d'ailleurs pas au seul volume de données recueillies, sans commune mesure avec ce que permet une interception de sécurité.

En effet, au contraire d'autres techniques de renseignement pour lesquelles la nature des éléments recueillis est inhérente à la technique mise en œuvre (le recours à une balise, par exemple, n'est susceptible de conduire à la fourniture que de données de localisation), le recueil de données informatiques recouvre des modalités d'action diverses, peut se concrétiser par de multiples dispositifs techniques et aboutir à des collectes de données très variées tant par leur ampleur que par leur nature ou leur qualité.

Par ailleurs, à l'inverse des techniques de renseignement faisant l'objet d'une centralisation au GIC qui sont, de fait, relativement standardisées, la pratique du recueil de données informatiques peut significativement différer selon le service qui y a recours, le type d'objectif concerné[47] ou encore les circonstances opérationnelles.

Ainsi, au-delà de la définition très générale de la technique donnée par la loi à l'article L. 853-2 du code de la sécurité intérieure, les modalités techniques précises de mise en œuvre des recueils de données informatiques dépendent de multiples facteurs : le type d'informations recherchées, la nature et les caractéristiques de l'équipement ciblé, les conditions et opportunités opérationnelles de mise en œuvre, les dispositifs employés ou encore les modes opératoires propres au service utilisateur.

À titre d'exemple, les moyens à mettre en œuvre pour recueillir des données sont nécessairement différents et présentent un caractère plus ou moins intrusif selon qu'elles sont contenues dans un support de stockage amovible appartenant à la personne ciblée ou au sein d'un réseau de machines compromises par un groupe de pirates informatiques étranger.

47. L'objectif désigne, au sens du 6° de l'article L. 821-2 du code de la sécurité intérieure, « *la ou les personnes, le ou les lieux ou véhicules concernés* ».

Cette hétérogénéité de la technique se retrouve également au stade de l'exploitation des données recueillies. Le type de support exploité, les outils mis en œuvre pour cette exploitation et les modalités pratiques d'exploitation propres à un service conduisent à de grandes différences au stade de la capitalisation tant dans la nature que dans le volume de données concernées, en particulier s'agissant des extractions[48].

Ainsi, dans l'hypothèse d'une attaque cyber évoquée précédemment, les services de renseignement font face à une importante variabilité et une forte complexité des modes opératoires à détecter et des traces sur lesquelles mener des investigations en renseignement. Le travail de capitalisation du service peut alors être séquentiel, par de multiples métiers, sur des supports et des réseaux aux fonctionnalités diverses. Cette complexité s'ajoute à la multiplicité des types de données collectées et des volumes engendrés par l'emploi de la technique de recueil de données informatiques. Il en résulte un contrôle particulièrement difficile pour la CNCTR y compris pour comprendre la démarche du service et parfois apprécier le lien avec la finalité invoquée.

3.1.2. L'année 2023 a donné lieu à des avancées importantes pour l'efficacité du contrôle. Certaines restent à concrétiser.

La poursuite d'un dialogue constructif avec les services et l'appui de la Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) ont permis au cours de l'année écoulée d'entériner des avancées significatives et d'enrayer à ce stade le risque d'un affaiblissement du contrôle. Trois chantiers sont à ce titre notables.

48. Mécanisme légal permettant la capitalisation de données brutes spécialement sélectionnées pour leur lien avec les finalités et les motifs visés par l'autorisation.

La levée de certains « angles morts »

En premier lieu, le dialogue technique instauré avec les services a conduit à lever plusieurs « angles morts » du contrôle *a posteriori* de la commission. L'accès à l'information s'est ainsi amélioré s'agissant des deux services qui représentent conjointement la majeure partie des données collectées permettant à la commission de disposer d'une vision élargie des conditions de recueil et d'exploitation utilisées.

La transmission de statistiques techniques permet à la CNCTR d'obtenir un état actualisé de la mise en œuvre des recueils autorisés et de mesurer le volume de données recueillies en amont de toute capitalisation par le service. Cette accélération de la mise à disposition des informations, autorisant la commission à anticiper ses contrôles sur pièces et sur place, lui permet de mieux cibler son intervention.

Par ailleurs, le contenu des éléments de traçabilité devant être établis par le service a été ajusté. Tout en préservant la confidentialité des modalités opérationnelles des services, les éléments de description supplémentaires fournis permettent d'améliorer la capacité de la CNCTR à analyser et interpréter les opérations effectuées et les informations recueillies. Ils facilitent la vérification de la corrélation entre la motivation fournie par le service au soutien de sa demande et la réalité de l'action qu'il a conduite sur le terrain une fois la technique autorisée.

Enfin, s'agissant de l'un des services du premier cercle, la réalisation d'évolutions techniques dans son système d'information interne a permis l'octroi à la commission d'un point d'accès unique pour examiner toutes les données stockées localement, accélérant ainsi l'exercice des contrôles sur pièces et sur place. Au-delà, la démarche menée par le service concerné a permis de sécuriser la gestion des données et l'application des délais de destruction, notamment en limitant la réalisation de copies manuelles et l'emploi de supports externes.

La commission se félicite donc du renforcement de ce dialogue technique avec les services, qu'elle appelait de ses vœux fin 2022, et des avancées concrètes qu'il a permises au cours de l'année 2023.

Un nouvel outil permettant une exploitation centralisée pour un champ encore restreint

Une possibilité nouvelle de centralisation des données recueillies a été ouverte par le GIC au cours de l'année 2023. Elle ne remet pas en cause la conservation des données pratiquée par les deux grands services utilisateurs mais elle offre aux autres services qui recourent, de manière plus ou moins fréquente au RDI, un outil d'exploitation centralisé pour certaines modalités de recueil.

À l'image du système d'information mis en place pour les interceptions de sécurité, cet outil, qui a vocation à évoluer, offre un cadre sécurisé pour l'intégration des données, leur manipulation et la réalisation d'opérations de transcriptions et d'extractions de données. La CNCTR bénéficie directement de ces travaux qui lui permettent un accès immédiat aux données collectées. Ainsi, un poste informatique directement attaché à ce réseau spécifique est installé depuis la fin 2023 dans les locaux de la commission.

Si des améliorations sont attendues pour permettre la mise en œuvre d'outils d'exploitation plus élaborés et plus fluides pour le travail des agents des services, la commission salue cette avancée, qui contribue en outre à une mutualisation des capacités techniques entre les services. Elle ne touche toutefois qu'une partie très minoritaire des RDI réalisés.

À plus long terme, un ambitieux projet de centralisation de l'ensemble des techniques de RDI garantissant à la commission un accès direct à l'ensemble des données recueillies

Le rapport d'activité pour l'année 2022 de la commission mettait l'accent sur la difficulté à contrôler l'usage des RDI et le risque de « décrochage » du contrôle qui en résultait. Conscient de ce risque, le Président de la République a demandé au Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) de susciter une réflexion commune aux deux services principalement intéressés (la direction générale de la sécurité intérieure, DGSI, et la direction générale de la sécurité extérieure, DGSE) sur une évolution des possibilités de contrôle.

Le projet finalement arrêté consiste à rassembler la totalité des données collectées sur les systèmes du GIC. La commission pourra ainsi y accéder à distance dans des conditions de sécurité garanties. Les services pourront eux-mêmes exploiter les données recueillies également à distance. Leurs conditions d'exploitation, non seulement ne seront pas dégradées, mais elles seront même améliorées car ce « GIC virtuel » mettra également à disposition les données recueillies par les traditionnelles écoutes téléphoniques que les services ne pouvaient jusqu'ici exploiter qu'en se déplaçant physiquement dans les locaux du GIC.

Les premières études de faisabilité démarreront au second semestre 2024 avec un objectif de mise en service des nouveaux outils courant 2027.

Dans l'attente de la concrétisation de ce projet indispensable à l'effectivité de la mission confiée à la commission, le dialogue technique régulier initié avec les services sera poursuivi pour empêcher tout décrochage du contrôle.

3.2. Un rendez-vous législatif en 2025 qui constitue une opportunité de faire évoluer le cadre légal vers un meilleur respect des exigences européennes et vers plus de cohérence et d'efficacité

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 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 que 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.

En l'absence de fixation du nombre maximal des autorisations d'interception par voie satellitaire pouvant être accordées simultanément, cette nouvelle technique n'a pas été mise en œuvre au cours de l'année 2023. Elle devrait l'être en 2024, laissant un temps limité pour en faire le bilan conformément à la demande du législateur.

Une nouvelle intervention législative est donc attendue au cours de l'année 2025, à tout le moins pour préciser l'avenir de cette technique. Cependant, dix ans après l'intervention des lois du 24 juillet 2015 et du 30 novembre 2015, ce rendez-vous législatif constitue une opportunité de faire évoluer les dispositions du code de la sécurité intérieure à la fois afin de mieux répondre aux exigences de la jurisprudence de la Cour européenne des droits de l'homme (CEDH) dans un contexte où devraient enfin intervenir les décisions sur les différentes requêtes, portant sur la loi du 24 juillet 2015, visant la France (3.2.1) mais également afin d'améliorer la cohérence interne et l'efficacité du régime alors adopté (3.2.2).

3.2.1. Une évolution du cadre légal serait nécessaire au regard des exigences de la jurisprudence européenne s'agissant en particulier des échanges avec les services étrangers et des fichiers dits de souveraineté alors que plusieurs arrêts concernant la France devraient intervenir en 2024

Comme la commission a eu l'occasion de l'évoquer à plusieurs reprises dans ses précédents rapports[49], quatorze requêtes introduites devant la CEDH entre le 7 octobre 2015 et le 21 avril 2017 et portant sur

49. Voir notamment les points 1.2.2 du 6ème rapport d'activité pour 2021 et le point 3.2.1 du 7ème rapport d'activité pour 2022, disponibles sur le site internet de la CNCTR.

les dispositions du code de la sécurité intérieure issues de la loi du 24 juillet 2015 sont actuellement toujours pendantes. Les décisions, d'abord annoncées pour l'année 2022 puis pour l'année 2023, ne sont pas encore intervenues à la date d'impression du présent rapport mais devraient l'être dans les prochaines semaines.

Pour mémoire, certains requérants soutiennent que les techniques de renseignement prévues par la loi ne satisfont pas aux exigences d'une base légale suffisante. Ils estiment ainsi que la notion d'« *informations ou documents* » pouvant être recueillis au moyen d'une technique de renseignement n'est pas définie et que la loi ne protège pas suffisamment les personnes exerçant la profession de journaliste ou d'avocat. Ils estiment en outre que le législateur a retenu une définition large des finalités légales pouvant fonder la mise en œuvre de mesures de surveillance, le régime légal ainsi créé n'étant pas, selon eux, « *strictement nécessaire à la préservation des institutions démocratiques* ».

Par ailleurs, les requérants se plaignent d'une insuffisance des garanties procédurales. Ils allèguent ainsi une absence de recours effectif en ce que, d'une part, le recours devant la CNCTR et le Conseil d'État ne remplirait pas les exigences de la Convention européenne des droits de l'homme et des libertés fondamentales (méconnaissance des principes d'équité, du contradictoire et de l'égalité des armes), d'autre part, qu'il est impossible de saisir directement le Conseil d'État des mesures de surveillance internationale ou du recueil et d'exploitation d'informations venant de services étrangers.

Or, à l'aune de la jurisprudence précédemment établie de la Cour en matière de renseignement, une évolution du cadre légal français apparaît inévitable.

En effet, les arrêts rendus par la grande chambre de la Cour le 25 mai 2021 (*Big Brother Watch et autres c. Royaume-Uni*[50] et *Centrum för rättvisa c. Suède*[51]) relatifs aux régimes de surveillance britannique et suédois l'ont conduite d'une part, à retenir que les dispositifs d'interception de masse des communications électroniques susceptibles d'être mise en place par les États parties devaient présenter des « garanties de bout en bout » et à préciser ces garanties[52]. Parmi celles-ci figurent l'organisation de la supervision par une autorité indépendante du respect des garanties énoncées et la mise en place d'un contrôle *a posteriori* indépendant ainsi que l'octroi de pouvoirs suffisants à l'organe compétent pour traiter d'éventuels manquements. D'autre part, la Cour a considéré que si le partage international de données entre services de renseignement étrangers pouvait être admis, il devait être encadré par des règles prévisibles et accessibles, présenter des garanties dans la gestion des données concernées et être soumis à un contrôle indépendant.

Ainsi, s'agissant de ces échanges avec les services étrangers, de nouvelles règles devraient être fixées dans le code de la sécurité intérieure pour limiter les flux sortants (renseignements susceptibles d'être transmis à un service étranger) aux données recueillies conformément aux dispositions de son livre VIII, les États destinataires devant justifier de garanties suffisantes en termes d'utilisation, de conservation et de non-divulgation des données[53]. En ce qui concerne les flux entrants (renseignements reçus de partenaires étrangers), ces règles devraient au moins interdire la réception de données

50. Voir CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n° 58170/13.

51. Voir CEDH, 25 mai 2021, *Centrum för rättvisa c. Suède*, n° 35252/08.

52. La Cour recherche en particulier si le cadre juridique national définit de façon suffisamment claire : les motifs pour lesquels l'interception en masse peut être autorisée ; les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ; la procédure d'octroi d'une autorisation ; les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ; les précautions à prendre pour la communication de ces éléments à d'autres parties ; les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ; les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ; et le es procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

53. La Cour retient qu'il appartient à un État transmetteur de s'assurer que l'organisme ou l'État destinataire des données a mis en place des règles permettant de garantir que le traitement de ces données ne fera pas l'objet d'abus ou d'ingérence disproportionnés, sans toutefois exiger que cet État destinataire présente des garanties strictement identiques à celles présentées par l'État transmetteur.

dont le recueil aurait été prohibé par la loi française. Par ailleurs, l'existence d'une supervision des échanges par une autorité indépendante serait nécessaire au moins lorsque ceux-ci interviennent avec un État qui n'est pas partie à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[54].

S'agissant des fichiers dits de souveraineté, le contrôle actuellement confié à la commission par les dispositions du code de la sécurité intérieure ne peut être regardé comme exhaustif en l'absence d'accès à tous les espaces de stockage de données des services au sein desquels il serait possible d'occulter les renseignements exclus du champ de sa compétence[55]. En outre, seul un tel accès est de nature à lui permettre de pleinement exercer son contrôle quand elle est saisie d'une réclamation sur le fondement de l'article L. 833-4 ou de l'article L. 854-9 du code étant souligné que les réponses formulées aux réclamants ne peuvent conduire à la révélation d'informations couvertes par le secret de la défense nationale. À cet égard, les entités de contrôle du cadre légal mises en place au sein des services, quand bien même les membres de cette structure interne bénéficieraient d'un statut particulier leur permettant de disposer d'une certaine autonomie, ne permettent pas de répondre aux exigences fixées par la CEDH qui prévoient que le contrôle doit être indépendant des autorités qui procèdent à la surveillance.

Enfin, s'agissant par ailleurs des modalités du droit au recours et plus particulièrement du principe du caractère contradictoire de la procédure, un meilleur respect des exigences européennes pourrait passer par une amélioration du dispositif actuel qui ne permet ni au requérant, ni à son conseil d'avoir connaissance de l'ensemble des éléments auxquels accèdent le Conseil d'État. À cet égard, à l'instar du modèle britannique de la « preuve secrète » rendue accessible uniquement à des avocats spécialement habilités[56], il pourrait être envisagé

54. En l'état, les dispositions du 4° de l'article L. 833-2 du code de la sécurité intérieure ne permettent pas à la CNCTR d'exiger un accès aux « *éléments communiqués par des services étrangers ou par des organismes internationaux* ».

55. Les dispositions du 4° de l'article L. 833-2 du code de la sécurité intérieure ne permettent notamment pas à la CNCTR d'exiger un accès aux éléments qui pourraient lui donner connaissance « *directement ou indirectement de l'identité des sources des services spécialisés du renseignement* ».

56. L'avocat spécialement habilité peut accéder aux preuves secrètes mais ne peut en révéler le contenu à son client.

la constitution d'un vivier d'avocats habilités au secret de la défense nationale auquel les requérants pourraient faire appel pour leur défense sans pouvoir eux-mêmes accéder à des informations relevant d'un tel secret.

Le rendez-vous législatif prévu en 2025, qui devrait intervenir après les décisions de la Cour concernant la France, constitue une opportunité pour faire évoluer le cadre légal français vers un meilleur respect des garanties énoncées par la jurisprudence de la Cour. Au-delà, il pourrait permettre d'améliorer la cohérence et l'efficience du cadre légal actuel sur divers points.

3.2.2. Des évolutions seraient également utiles pour améliorer la cohérence et l'efficience du cadre légal actuel

Après près de 10 ans d'application des lois de 2015, il apparaît que certaines techniques qui avaient suscité beaucoup d'inquiétudes se révèlent en pratique, ou au regard de l'utilisation qui peut effectivement en être faite par les services, moins attentatoires aux libertés publiques que d'autres techniques qui avaient pourtant moins fait débat. Il en résulte qu'un contingentement ou un encadrement plus strict a parfois été prévu pour des techniques moins intrusives que d'autres pour lesquelles un tel contingentement ou encadrement n'a pas été prévu par la loi.

Ainsi, les dispositions du II de l'article L. 851-2 du code de la sécurité intérieure prévoient un contingentement des accès aux données techniques de connexion en temps réel et limitent cette technique à la prévention du terrorisme alors que le recueil de données informatiques prévu à l'article L. 853-2 du même code, qui permet pourtant d'accéder à une masse très importante de données, le cas échéant, selon des modalités très intrusives[57.58], n'est pas contingenté

57. Voir point 3.1 ci-dessus.

58. De même, les techniques de captation d'images ou de captation de sons prévues à l'article L. 853-1 du code de la sécurité intérieure ne sont pas soumises à un contingent.

et accessible au titre de toutes les finalités mentionnées à l'article L. 811-3. Au-delà, l'absence de possibilité de recourir à l'accès aux données en temps réel pour certaines finalités, telle que la prévention des violences collectives, conduit à devoir envisager plus rapidement le recours à des techniques plus intrusives.

Selon la même logique, les dispositions relatives à la surveillance internationale prévoient un encadrement très spécifique des mesures susceptibles de viser des identifiants rattachables au territoire national (IRTN). Cependant, l'absence de définition légale de la notion et son ambivalence, de même que le silence de la loi s'agissant du traitement des identifiants non-rattachables au territoire national peut paradoxalement aboutir à une protection renforcée de ces derniers alors que telle ne semblait pas être l'intention du législateur de la loi du 20 novembre 2015[59].

Par ailleurs, afin de clarifier la portée de certaines dispositions, de sécuriser l'intervention des services de renseignement mais aussi de conforter les garanties apportées aux citoyens, certaines autres notions mériteraient d'être mieux précisées.

Ainsi, pour les motifs exposés dans le cadre de l'étude figurant au présent rapport[60], la notion d'entourage, introduite initialement à l'article L. 852-1 du code de la sécurité intérieure, pourrait être plus explicite sans référence à l'éventuelle surveillance mise en œuvre à l'égard de la cible principale.

De même, en matière de réclamations et de recours, les dispositions des articles L. 833-4 et L. 841-1 du code de la sécurité intérieure mériteraient une clarification s'agissant de l'étendue des vérifications à opérer dans le temps.

En effet, en l'état, la commission effectue des vérifications des traces en remontant jusqu'à la date d'entrée en vigueur de la loi du 24 juillet 2015

59. Voir notamment les dispositions relatives aux vérifications ponctuelles prévues à l'article L. 854-2 du code de la sécurité intérieure.
60. Voir étude 2 ci-dessous.

s'agissant de la surveillance domestique mais le délai s'écoulant depuis l'intervention de cette loi doit conduire à s'interroger sur l'opportunité de fixer une limite en la matière. Par ailleurs, alors que les dispositions du II de l'article L. 822-2 du code de la sécurité intérieure prévoient que les renseignements qui concernent une requête dont le Conseil d'État a été saisi ne peuvent être détruits et doivent être conservés pour les seuls besoins de la procédure devant cette juridiction, des dispositions équivalentes ne sont pas prévues s'agissant des réclamations adressées à la CNCTR en vertu de l'article L. 833-4 ou de l'article L. 854-9 du même code, de sorte qu'entre l'intervention d'une telle réclamation, la réponse de la commission et une éventuelle saisine du Conseil d'État des données auront pu être supprimées.

Enfin, certaines évolutions seraient utiles afin de rendre plus fluide ou plus efficace l'intervention de la commission.

Ainsi, par exemple, la combinaison des dispositions des articles L. 831-2[61] et du deuxième alinéa de l'article L. 832-3[62] conduit en l'état à imposer les conditions de quorum de la formation plénière à des demandes relevant en pratique de la compétence de la formation restreinte dès lors qu'au moins un membre parlementaire est présent dans la composition.

Également, les demandes d'introduction dans un lieu privé à usage d'habitation aux fins de retrait ou de maintenance d'un dispositif déjà autorisé par la formation collégiale doivent être examinés soit par cette même formation, soit par un membre seul ayant la qualité de magistrat. Cependant, dans ce dernier cas, la formation collégiale plénière doit être informée. Cette information pourrait être supprimée ou, à tout le moins, pouvoir être portée devant la formation collégiale restreinte.

Selon la même logique, mais sans incidence concrète supplémentaire pour les libertés publiques, certaines règles de recours aux techniques

61. « *La formation plénière de la Commission nationale de contrôle des techniques de renseignement comprend l'ensemble des membres mentionnés à l'article L. 831-1. / La formation restreinte de la Commission nationale de contrôle des techniques de renseignement est composée des membres mentionnés aux 2° à 4° du même article L. 831-1. / (...)* ».

62. « *(...) La formation restreinte et la formation plénière ne peuvent valablement délibérer que si, respectivement, au moins trois et quatre membres sont présents. (...)* ».

ou d'encadrement de ces dernières mériteraient d'être harmonisées par souci de cohérence et d'efficacité.

Il en va notamment ainsi de la durée d'autorisation de l'introduction dans un lieu privé (ILP), fixée à 30 jours par le III de l'article L. 853-3 du code de la sécurité intérieure par dérogation aux dispositions de l'article L. 821-4 du même code. L'ILP ne constitue en effet pas une technique en tant que telle, mais le support nécessaire à la mise en œuvre d'une autre technique telle que la captation d'images ou de sons ou encore le recueil de données informatiques. Or, les durées d'autorisation de ces techniques sont plus longues que celle prévue pour l'ILP (deux mois maximum en vertu du II respectivement de l'article L. 853-1 et de l'article L. 853-2 du code de la sécurité intérieure), de sorte qu'il arrive régulièrement qu'une demande de renouvellement d'ILP soit nécessaire afin de permettre la mise en œuvre d'une technique par ailleurs toujours autorisée mais qui, en pratique, n'a pas pu être installée.

Dans le même sens, la formulation du contingent prévu à l'article L. 851-6 du code de la sécurité intérieure s'agissant des appareil ou d'un dispositif permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés (*IMSI-catcher*) pourrait être revue afin de viser le nombre d'autorisations accordées simultanément et non le nombre de dispositifs pouvant être utilisés simultanément qui rend en pratique le contrôle de la commission sur le respect de ce contingent très difficile voire impossible.

Études :
Les zones grises de la surveillance

Étude 1. Contours et enjeux de la surveillance au titre de la prévention de la criminalité et de la délinquance organisées

Le code de la sécurité intérieure prévoit que le recours aux techniques de renseignement ne peut être autorisé que pour la défense ou la promotion d'un nombre limité d'intérêts fondamentaux. Ces intérêts fondamentaux sont énumérés à son article L. 811-3, qui distingue sept finalités[1] parmi lesquelles figure à son 6° : « *La prévention de la criminalité et de la délinquance organisées* ».

Cette finalité, dont le champ d'application a été défini par référence à des infractions pénales justifiant le recours à une procédure et à des techniques d'enquête dérogeant au droit commun, présente donc une spécificité tenant au fait que les techniques de surveillance administrative, si elles sont productives, doivent aboutir à la saisine de l'autorité judiciaire, de sorte que la question de l'articulation entre procédures administrative et judiciaire se trouve particulièrement, voire nécessairement posée.

La notion de « criminalité et délinquance organisées » au sens de cette finalité ne recouvre cependant pas l'ensemble des infractions aggravées par la circonstance de bande organisée au sens du code pénal, ni l'ensemble des infractions susceptibles d'entrer dans le champ de la procédure applicable à la criminalité et à la délinquance

1. Les autres finalités mentionnées à l'article L. 811-3 sont, au 1° de cet article, l'indépendance nationale, l'intégrité du territoire et la défense nationale, 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, à son 3° Les intérêts économiques, industriels et scientifiques majeurs de la France, à son 4° La prévention du terrorisme, 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, et à son 7° La prévention de la prolifération des armes de destruction massive.

organisées au sens du code de procédure pénale. La CNCTR, à l'aune de la jurisprudence du Conseil constitutionnel, a donc été conduite à en préciser le périmètre (1).

Par ailleurs, cette finalité est plus particulièrement susceptible de soulever des difficultés en matière de respect des champs d'intervention respectifs de la police administrative et de l'autorité judiciaire. A travers ses avis sur les demandes de techniques de recueil de renseignement, la commission a donc également été conduite à délimiter plus précisément le champ d'intervention du renseignement administratif. Elle s'efforce à cet égard de favoriser le dialogue entre les services de renseignement et l'autorité judiciaire afin d'améliorer l'articulation entre procédures administrative et judiciaire (2).

1. Une finalité au périmètre différent de l'acception de la notion de délinquance et criminalité organisées au sens du droit pénal

La notion de délinquance et de criminalité organisées est à l'origine définie par le code pénal. Elle a conduit à prévoir des adaptations de la procédure pénale de droit commun (1.1). Cependant, la finalité de la prévention de la délinquance et de la criminalité organisées au sens du code de la sécurité intérieure recouvre un périmètre plus restreint que la CNCTR est venue préciser à la suite des interprétations données par le Conseil constitutionnel dans sa décision n° 2015-713 DC du 23 juillet 2015 portant sur la loi relative au renseignement (1.2).

1.1. La notion de délinquance et de criminalité organisées au sens pénal présente plusieurs acceptions

Au sens du droit pénal et de la procédure pénale, la délinquance et la criminalité organisées peuvent correspondre aux infractions commises en bande organisée (1.1.1), mais également à celles pour lesquelles le législateur a prévu un régime procédural dérogatoire au droit commun (1.1.2) ou la compétence de juridictions spécialisées (1.1.3).

1.1.1. | La notion de bande organisée au sens du code pénal

En droit pénal, la notion de bande organisée correspond à une circonstance aggravante, qui doit être prévue par la loi et qui a pour conséquence l'augmentation du quantum de la peine encourue. La circonstance aggravante de commission en bande organisée n'existe pas pour toutes les infractions pénales.

Dans son article 132-71, le code pénal prévoit que : « *Constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions* ». Cette définition est identique à celle de l'infraction d'association de malfaiteurs[2].

Il résulte toutefois de la jurisprudence du Conseil constitutionnel que la bande organisée implique une préméditation et une organisation structurée[3]. La Cour de cassation a également précisé que la notion de bande organisée impliquait une logistique et une répartition des tâches entre ses membres[4].

2. Voir l'article 450-1 du code pénal.
3. Voir la décision n° 2004-492 DC du 2 mars 2004, considérant 13.
4. Voir Cass. Crim, 8 juillet 2015, n° 14-88.329, bull. crim., n° 834.

1.1.2. Les régimes procéduraux dérogatoires applicables à certaines infractions relevant de la délinquance et de la criminalité organisées

La loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité organisée, dite « Perben II », a créé un régime procédural dérogatoire au droit commun pour certaines infractions, dans l'objectif de lutter plus efficacement contre les trafics et le crime organisé. Le titre XXV du livre IV du code de procédure pénale institue ainsi des règles particulières de compétence, avec la création de juridictions spécialisées, et de procédure, permettant de déroger aux règles de droit commun applicables à la garde à vue, aux perquisitions et aux mesures conservatoires notamment. Il autorise également le recours à des « techniques spéciales » d'enquête.

Dans son article 706-73, le code de procédure pénale énumère les infractions qui permettent l'application de l'ensemble de ces règles dérogatoires au droit commun. Ainsi, ces infractions sont susceptibles de justifier notamment le recours, dès le stade de l'enquête préliminaire, à des interceptions de correspondances, à la captation d'images ou de paroles dans des lieux privés, à un *IMSI-catcher* ou encore à la captation de données informatiques, soit des techniques similaires ou comparables à certaines techniques prévues par le code de la sécurité intérieure pour le renseignement administratif.

Les infractions visées par cet article relèvent, selon la circulaire[5] présentant les dispositions de la loi du 9 mars 2004, de la « grande délinquance organisée ». Si certaines de ces infractions doivent être commises avec la circonstance aggravante de bande organisée

5. Voir notamment la circulaire du 2 septembre 2004 de présentation des dispositions relatives à la criminalité organisée de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

pour entrer dans le champ de l'article 706-73, tel le crime de meurtre[6], ce n'est pas le cas pour d'autres, tels les crimes et délits de trafic de stupéfiants[7], les crimes et délits aggravés de traite des êtres humains[8] ou encore les crimes et délits aggravés de proxénétisme aggravé[9], qui comportent intrinsèquement une notion d'organisation criminelle.

L'article 706-73-1 du code de procédure pénale énumère pour sa part les infractions, principalement économiques et financières (notamment les délits d'escroquerie ou de dissimulation d'activités ou de salariés en bande organisée[10], ou encore les délits de trafic de biens culturels[11]), qui, entrant dans le champ de la criminalité et de la délinquance organisées, permettent l'application de l'ensemble des règles dérogatoires au droit commun à l'exception de celles régissant la garde à vue[12]. Cet article a été introduit dans le code de procédure pénale par la loi n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne, à la suite d'une décision du Conseil constitutionnel ayant jugé contraire à la Constitution le 8° bis de l'article 706-73 du code de procédure pénale qui visait l'escroquerie en bande organisée[13]. Le Conseil constitutionnel a considéré que ce délit n'étant pas susceptible « *de porter atteinte en lui-même à la sécurité, à la dignité ou à la vie des personnes* », le régime dérogatoire de la garde à vue prévu par le législateur constituait une atteinte disproportionnée à la liberté individuelle et aux droits de la défense par rapport au but poursuivi.

Les infractions qui ne sont citées ni par l'article 706-73, ni par l'article 706-73-1 du code de procédure pénale et qui sont commises

6. Voir le 1° de l'article 706-73 du code procédure pénale.
7. Voir le 3° de l'article 706-73 du code procédure pénale.
8. Voir le 5° de l'article 706-73 du code procédure pénale.
9. Voir le 6° de l'article 706-73 du code procédure pénale.
10. Voir les1° et 2° de l'article 706-73-1 du code de procédure pénale.
11. Voir le 6° de l'article 706-73-1 du code de procédure pénale
12. Ne sont ainsi pas applicables à ces infractions les dispositions de l'article 706-88 du code de procédure pénale qui permettent notamment de porter la durée de la garde à vue jusqu'à 96h et de reporter l'intervention de l'avocat.
13. Voir la décision n° 2015-508 QPC du 11 décembre 2015, M. Amir F. *[Prolongation exceptionnelle de la garde à vue pour des faits de blanchiment, de recel et d'association de malfaiteurs en lien avec des faits d'escroquerie en bande organisée]*, considérant 13.

en bande organisée relèvent du régime prévu par l'article 706-74 du même code. S'agissant de ces infractions, le périmètre des règles dérogatoires au droit commun est beaucoup plus restreint puisque seules deux techniques spéciales d'enquête sont applicables : l'extension de compétence des officiers et, le cas échéant, des agents de police judiciaire à l'ensemble du territoire national afin de poursuivre la surveillance de personnes ou du transport de biens[14] et les mesures conservatoires des avoirs criminels[15]. Ainsi, aucune technique spéciale d'enquête comparable aux techniques de renseignement ne peut être mise en œuvre.

Parallèlement à ces dispositions du code de procédure pénale, le dernier alinéa de l'article 414 du code des douanes réprime les délits de contrebande et d'importation ou d'exportation sans déclaration de marchandises prohibées en bande organisée. Le régime procédural applicable à ces infractions est celui prévu par le code des douanes qui comporte également des procédures spéciales d'enquête. Ces infractions ont par ailleurs récemment été ajoutées à celles mentionnées à l'article 706-73 du code de procédure pénale par loi n° 2023-610 du 18 juillet 2023 visant à donner à la douane les moyens de faire face aux nouvelles menaces[16].

1.1.3. | Les infractions relevant de juridictions spécialisées

En plus de celles déjà mentionnées, d'autres infractions peuvent donner lieu à l'application du régime procédural dérogatoire prévu pour la criminalité et la délinquance organisées dès lors que leur complexité justifie qu'elles relèvent de la compétence de certaines juridictions spécialisées.

Ainsi, l'article 706-1-1 du code de procédure pénale prévoit que certaines infractions relevant de la compétence du parquet national financier[17]

14. Voir les articles 706-80 et suivants du code de procédure pénale.
15. Voir l'article 706-103 du code de procédure pénale.
16. Voir l'article 29 de la loi insérant un 21° à l'article 706-73 du code de procédure pénale.
17. Voir les articles 705 et suivants du code de procédure pénale.

peuvent donner lieu à l'application de l'ensemble des règles dérogatoires au droit commun à l'exception de celles relative à la garde à vue et aux perquisitions en dehors des heures légales[18]. Ce régime est notamment applicable au délit de corruption, au trafic d'influence, ou au détournement de fonds (sans exigence de la circonstance de bande organisée), ainsi qu'à la fraude fiscale et à la prise illégale d'intérêts lorsqu'elles sont commises en bande organisée.

Certaines infractions relevant de la compétence des pôles de santé publique, notamment le trafic de médicaments aggravé, peuvent également se voir appliquer un régime d'enquête dérogatoire, bien que plus restrictif que celui précédemment évoqué[19].

Au sens du droit pénal et de la procédure pénale, la notion de délinquance et de criminalité organisées recouvre donc une pluralité d'infractions plus ou moins graves relevant de régimes procéduraux distincts.

1.2. La notion de délinquance et de criminalité organisées au sens du code de la sécurité intérieure est plus restrictive

1.2.1. L'interprétation stricte retenue par l'ancienne Commission nationale de contrôle des interceptions de sécurité (CNCIS) dans le cadre de la loi du 10 juillet 1991

Dès l'intervention de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications[20],

18. Voir les articles 706-89 à 706-94 du code de procédure pénale.
19. Voir l'article 706-2-2 du code de procédure pénale.
20. Voir l'article 3 de la loi, codifié par la suite à l'article 241-2 du code de la sécurité intérieure.

la prévention de la délinquance et de la criminalité organisées a figuré parmi les finalités permettant la mise en œuvre d'interceptions de sécurité aux fins de renseignement.

Amenée à préciser le champ d'application de cette finalité, la CNCIS avait considéré, avant l'introduction d'un régime procédural dérogatoire applicable à la criminalité et à la délinquance organisées dans le code de procédure pénale, qu'étaient susceptibles d'être présentées au titre de la finalité de la prévention de la criminalité et délinquance organisées, les demandes concernant non seulement les infractions commises en bande organisée, mais également celles supposant un certain degré d'organisation, c'est-à-dire une certaine distribution des rôles[21].

Après l'intervention de la loi du 9 mars 2004 précitée, la commission avait retenu une définition de la finalité recouvrant « *totalement le champ couvert par l'article 706-73 du code de procédure pénale* » excluant de ce fait « *l'essentiel des infractions financières commises en bande organisée* [relevant] *en grande majorité de l'article 706-74 du code de procédure pénale* ». Elle admettait néanmoins d'inclure dans le champ de la finalité des infractions qui, bien que non visées par l'article 706-73, étaient de nature à porter atteinte à la vie ou de manière grave, à la santé publique. Elle avait ainsi estimé s'agissant de ces infractions que « *l'ampleur du trafic présumé, les modalités de commission des infractions projetées (notamment leur aspect international), les risques d'atteinte à la santé des victimes* » présentaient des effets « comparables » aux intérêts protégés par les incriminations de l'article 706-73, justifiant des avis favorables au cas par cas « dans la mesure où les faits revêtaient le caractère exceptionnel fixé par la loi pour autoriser une interception de sécurité » [22].

21. Voir le rapport d'activité 2002 de la CNCIS, p. 68 à 72.
22. Voir le rapport d'activité 2014-2015 de la CNCIS, p. 130-131.

1.2.2. Une interprétation confortée par l'intervention de la loi du 24 juillet 2015 et éclairée par la décision du Conseil constitutionnel du 23 juillet 2015

Au cours des débats parlementaires relatifs à la loi du 24 juillet 2015 relative au renseignement, le Gouvernement s'est opposé à un amendement ayant pour objet de limiter le champ d'application de la finalité par rapport à ce qui était auparavant prévu à l'article L. 241-2 du code de la sécurité intérieure en le restreignant aux crimes et délits punis d'au moins cinq ans d'emprisonnement. Il avait fait valoir que les termes « criminalité et délinquance organisées » se référaient, ainsi que l'avaient montré les avis de la CNCIS, aux infractions visées à l'article 706-73 du code de procédure pénale, toutes réprimées par une peine privative de liberté supérieure à cinq ans[23].

Dans sa décision du 23 juillet 2015[24], le Conseil constitutionnel, alors qu'était invoqué le caractère trop large et insuffisamment défini des finalités énumérées au nouvel article L. 8113 du code de la sécurité intérieure, a considéré que le législateur avait précisément circonscrit la finalité mentionnée au 6° de cet article et retenu des critères en adéquation avec l'objectif poursuivi en faisant référence « *aux incriminations pénales énumérées à l'article 706-73 du code de procédure pénale et aux délits punis par l'article 414 du code des douanes commis en bande organisée* ».

Cette référence aux dispositions du dernier alinéa de l'article 414 du code des douanes ne figure pas dans les débats parlementaires mais apparaît en revanche dans les observations présentées par le Gouvernement devant le Conseil constitutionnel[25] en cohérence avec le régime procédural applicable aux infractions concernées.

23. Voir le compte-rendu des débats en séance publique à l'Assemblée nationale (1ère lecture), deuxième séance du 13 avril 2015, sur l'amendement n° 108 présenté par M. Morin et autres le 9 avril 2015 (rejeté).

24. Voir la décision n° 2015-713 DC du 23 juillet 2015, considérant 10.

25. Voir les observations du Gouvernement devant le Conseil constitutionnel aux termes desquelles : « *la notion de délinquance et de criminalité organisées renvoie aux dispositions prévues par l'article 706-73 du CPP qui liste des crimes et délits permettant l'utilisation des techniques spéciales d'enquête, ainsi qu'aux délits punis par l'article 414 du code des douanes lorsqu'ils sont commis en bande organisée* ».

1.2.3. L'impact des modifications ultérieures du droit pénal et de la procédure pénale

La CNCTR s'est efforcée de construire une doctrine permettant de délimiter les contours de cette finalité en interprétant la portée des différentes interventions ultérieures du législateur conduisant à créer de nouvelles infractions ou à instaurer de nouvelle règles de procédure dans le champ de la délinquance et de la criminalité organisées, à l'aune de la décision du Conseil constitutionnel du 23 juillet 2015.

À cet égard, elle a considéré que cette décision n'avait ni pour objet, ni pour effet de « cristalliser » la liste des infractions dont la prévention est susceptible de justifier la mise en œuvre d'une technique de renseignement en la limitant aux infractions mentionnées à l'article 706-73 du code de procédure pénale dans sa rédaction en vigueur à la date de la décision du Conseil constitutionnel.

Elle retient en conséquence un double critère matériel tenant, d'une part, à la réalité d'une action « en bande organisée », conformément à l'approche du Conseil constitutionnel et la jurisprudence de la Cour de cassation, et d'autre part, au degré de gravité ou de dangerosité de la menace qu'il s'agit de prévenir, justifiant le recours à des techniques de surveillance en amont d'une éventuelle procédure judiciaire. Elle prend également en compte un élément procédural en recherchant si des techniques spéciales d'enquête, assimilables aux techniques relevant du code de la sécurité intérieure, sont susceptibles d'être mises en œuvre pour la recherche, la constatation et la poursuite de ces infractions.

Ainsi, s'agissant des infractions qui ne sont pas couvertes par les dispositions auxquelles s'est expressément référé le Conseil constitutionnel dans sa décision du 23 juillet 2015, la CNCTR considère que l'usage de techniques de renseignement pour la prévention de la délinquance et de la criminalité organisées au sens du code de la sécurité intérieure

ne peut concerner que des infractions qui, à l'instar de celles mentionnées aux articles 706-73 du code de procédure pénale et 414 du code des douanes, relèvent de la « grande délinquance organisée ».

La commission a dès lors estimé que les infractions mentionnées à l'article 706-73-1 du code de procédure pénale[26], qui a été introduit dans le droit positif postérieurement à l'intervention de la décision du Conseil constitutionnel du 23 juillet 2015[27], entraient également dans le champ de cette finalité.

En effet, les infractions commises avec la circonstance de la bande organisée présentent un important degré de gravité et le régime procédural dérogatoire au droit commun qui leur est applicable est quasiment identique à celui prévu pour les infractions mentionnées à l'article 706-73 du code de procédure pénale. L'ensemble des techniques spéciales d'enquête, particulièrement attentatoires à la vie privée applicables aux infractions mentionnées à l'article 706-73 leur sont également applicables.

A contrario, la commission considère que la prévention des infractions qui, bien que commises avec la circonstance de bande organisée au sens du code pénal, relèvent du régime prévu par l'article 706-74 du code de procédure pénale (par exemple s'agissant du trafic de faux documents en bande organisée) ne permet pas l'usage de techniques de renseignement. D'une part, l'article 706-74 du code de procédure pénale avait déjà été introduit dans le droit positif à la date à laquelle la décision du Conseil constitutionnel du 23 juillet 2015 est intervenue et il comportait des dispositions similaires à celles actuellement en vigueur s'agissant du régime procédural dérogatoire au droit commun applicable. D'autre part, le régime applicable aux infractions mentionnées à l'article 706-74 est largement comparable à celui prévu pour les infractions de droit commun, ne permettant le recours qu'à un nombre limité de techniques spéciales d'enquête.

26. Telles que le délit d'escroquerie en bande organisée ou les délits de dissimulation d'activités ou de salariés, de recours aux services d'une personne exerçant un travail dissimulé, de marchandage de main-d'œuvre, de prêt illicite de main-d'œuvre ou d'emploi d'étranger sans titre de travail, commis en bande organisée.

27. Voir point 1.1.2 ci-dessus.

De même, la commission n'a pas estimé possible d'étendre le périmètre de la « finalité 6 » aux infractions susceptibles de relever des juridictions spécialisées telles que le parquet national financier (par exemples les délits de corruption, de trafic d'influence, ou de prise illégale d'intérêts, ou encore le délits d'initiés) ou les pôles de santé publique (trafic de produits dopants). Quand bien même le régime procédural applicable à ces infractions permet la mise en œuvre de techniques d'enquête particulièrement intrusives, elle a constaté que les dispositions de l'article 706-1-1 du code de procédure pénale, qui mentionnent diverses infractions en matière économique et financière, étaient déjà en vigueur à la date à laquelle la décision du Conseil constitutionnel est intervenue et qu'elles avaient donc volontairement été exclues du champ d'application de la « finalité 6 ».

S'agissant des personnes susceptibles d'être visées par des techniques de renseignement sur le fondement de la finalité tendant à la prévention de la délinquance et de la criminalité organisées, en cohérence avec l'exigence de « *présomption d'implication directe et personnelle* »[28] à l'aune de laquelle sont examinées les demandes qui lui sont adressées, la CNCTR estime que seules les personnes susceptibles d'être impliquées en qualité d'auteur ou de complice des infractions entrant dans le champ de la finalité peuvent faire l'objet de telles techniques. Elle a en conséquence pu rendre des avis défavorables sur des demandes portant sur une victime supposée de faits proxénétisme ou encore à l'égard d'un usager de produits stupéfiants faute d'éléments permettant de retenir l'implication éventuelle de cet usager dans un trafic.

28. Voir l'étude 2 du présent rapport « Surveiller l'entourage ? » ci-dessous.

2. Une finalité qui présente un enjeu particulier pour le respect du champ d'intervention de la police administrative par rapport aux procédures judiciaires

La commission veille également à ce que l'action des services de renseignement dans le champ de la prévention de la délinquance et de la criminalité organisées n'empiète pas sur les prérogatives de l'autorité judiciaire compétente pour la recherche et la poursuite des infractions.

En effet, dans sa décision du 23 juillet 2015 précitée, si le Conseil constitutionnel a considéré que le législateur avait précisément circonscrit les contours de la finalité tendant à la prévention de la délinquance et de la criminalité organisées, il a au préalable rappelé que le recueil de renseignement au moyen des techniques définies au titre V du livre VIII du code de la sécurité intérieure, qui relève de la police administrative, ne pouvait avoir « *d'autre but que de préserver l'ordre public et de prévenir les infractions* » et, par suite, qu'il ne pouvait être mis en œuvre « *pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs* »[29].

Par ses avis, la CNCTR s'est donc attachée à dégager une doctrine destinée à garantir le respect des champs d'intervention respectifs de la police administrative et de l'autorité judiciaire (2.1).

Cependant, l'examen des demandes dont la commission est saisie sur le fondement de la « finalité 6 » a mis en évidence la nécessité, pour assurer concrètement ce respect, d'un dialogue étroit entre la communauté du renseignement et l'autorité judiciaire. L'évolution des contentieux de la grande délinquance et de la criminalité organisées rend en effet aujourd'hui cruciale la mise en œuvre d'une articulation réelle, souple et efficiente entre les champs administratif et judiciaire (2.2).

29. Voir décision précitée, considérant 9.

2.1. La nécessaire délimitation du champ d'intervention de la surveillance administrative par rapport aux procédures judiciaires

2.1.1. Les principes de séparation des pouvoirs et de respect du champ d'intervention de l'autorité judiciaire

Le contrôle de légalité réalisé par la commission dans le cadre de l'examen des demandes de techniques de renseignement dont elle est saisie inclut nécessairement un contrôle du respect du principe de séparation des pouvoirs tel qu'explicité par le Conseil constitutionnel dans sa décision du 23 juillet 2015 précitée, dont découle le respect des champs d'intervention respectifs de la police administrative et de l'autorité judiciaire en la matière. Le recueil de renseignements au moyen des techniques mentionnées dans le code de la sécurité intérieure ne peut ainsi avoir pour but que de préserver l'ordre public et de prévenir les infractions. La police judiciaire est pour sa part seule compétente pour constater les infractions à la loi pénale, en rassembler les preuves et en rechercher les auteurs.

L'examen par la commission des demandes de techniques de renseignement présentées sur le fondement de la « finalité 6 » est ainsi particulièrement attentif tant s'agissant des textes d'incrimination visés par le service au soutien de sa demande[30] que s'agissant des faits dont le service entend prévenir la commission et le stade de leur caractérisation.

30. Une même demande a ainsi pu recevoir, successivement, un avis défavorable faute de faire mention d'une base légale entrant dans le champ de la finalité, puis favorable dès lors que le dernier alinéa de l'article 414 du code des douanes a été mentionné. La CNCTR a à cet égard admis qu'un service de renseignement autre que la Direction nationale du renseignement et des enquêtes douanières (DNRED) sollicite des techniques de renseignement afin de prévenir la menace liée à un trafic qui relèverait des dispositions de l'article 414 du code des douanes (sans être mentionné par les dispositions des articles 706-73 et 706-73-1 du code de procédure pénale), dès lors que les éléments permettent de soupçonner que les faits sont commis en bande organisée.

La CNCTR s'attache en particulier à s'assurer de l'absence d'infraction pénale d'ores et déjà constatée qui justifierait la saisine immédiate de l'autorité judiciaire et appellerait en conséquence un avis défavorable à la mise en œuvre de techniques de surveillance administrative.

Elle veille ainsi à ce que la « finalité 6 » ne soit pas invoquée de manière « détournée », pour permettre le recours à une technique de renseignement prévue par le code de la sécurité intérieure dans une hypothèse où la possibilité de recourir à la technique spéciale d'enquête similaire prévue par le code de procédure pénale apparaîtrait plus incertaine au service.

La commission est aussi particulièrement vigilante dans les hypothèses où des « allers-retours » entre les cadres administratif et judiciaire interviennent, par exemple lorsqu'une enquête judiciaire est ouverte sur la base d'un renseignement administratif aux fins de mise en œuvre des techniques spéciales d'enquête prévues par le code de procédure pénale, puis clôturée aux fins d'ouverture d'une nouvelle phase administrative sur le fondement du code de la sécurité intérieure destinée à permettre *in fine* l'ouverture d'une enquête judiciaire. Ces configurations sont en effet porteuses d'un risque procédural majeur tant au regard du principe de légalité que du principe de loyauté dans le recueil de la preuve.

2.1.2. Une frontière parfois difficile à tracer qui a conduit la CNCTR à adapter ses avis

En pratique, le moment précis où le temps de la prévention est achevé parce que l'infraction a reçu un commencement d'exécution peut être délicat à caractériser.

La commission prend toutefois en compte la « divisibilité » possible de la surveillance. Ainsi, lorsque certaines conditions sont réunies,

elle peut rendre des avis favorables même dans des hypothèses où l'autorité judiciaire est saisie ou serait susceptible de l'être. Ces avis favorables sont toutefois assortis d'une restriction « à l'exception des faits dont l'autorité judiciaire est saisie » ayant pour conséquence d'interdire au service de rechercher des éléments en lien avec les infractions faisant déjà l'objet d'une procédure judiciaire ou dont l'autorité judiciaire devrait se saisir de façon imminente.

En pratique, deux hypothèses peuvent être distinguées à ce titre :

- la demande fait état d'infractions dont l'autorité judiciaire est déjà saisie, mais dont la nature ou le contexte dans lequel elles ont été commises rendent particulièrement vraisemblable une réitération de la part de la cible que le service entend prévenir ;

- la cible fait l'objet de poursuites judiciaires pour certains faits, mais le service fait état dans sa demande de faits distincts et recouvrant une qualification pénale différente, dans laquelle cette cible serait susceptible d'être également impliquée.

Par ailleurs, alors que des éléments permettent de considérer que la caractérisation d'une infraction se dessine, le service peut être en mesure d'indiquer qu'il a déjà communiqué les renseignements en sa possession à l'autorité judiciaire, le cas échéant dans le cadre des dispositions de l'article 40 du code de procédure pénale, pour permettre l'ouverture d'une enquête judiciaire, mais que cette dernière ne s'est, en l'état, pas saisie. Dans cette dernière hypothèse, la commission peut être amenée à rendre un avis favorable « *pour confirmer l'implication personnelle de la cible en lien avec le motif demandé* » ou pour une dernière surveillance avant saisine de l'autorité judiciaire.

Ce souci de pragmatisme ne doit pas cacher la nécessité d'un dialogue plus construit entre les services de renseignement et l'autorité judiciaire, tant pour s'assurer de l'effectivité du respect du principe de séparation des pouvoirs que pour permettre d'entraver la très grande criminalité organisée de la manière la plus efficiente possible.

2.2. La nécessité d'améliorer les échanges entre les services de renseignement, la commission et l'autorité judiciaire afin d'éviter des difficultés néfastes pour leurs missions respectives

2.2.1. | Un besoin commun de concertation

Le développement d'une meilleure concertation entre, d'une part, la commission et les services de renseignement, d'autre part, les services de renseignement et l'autorité judiciaire, répond à un double objectif de protection des capacités opérationnelles des services et de sécurisation des procédures pénales.

Il s'agit ainsi, en renforçant la maîtrise et la fluidité de l'articulation entre services de renseignement et autorité judiciaire de favoriser l'action des services de renseignement là où elle se justifie, dans un objectif final d'entrave judiciaire. Il s'agit aussi, en déterminant le moment le plus opportun pour opérer la bascule du cadre administratif vers le cadre judiciaire de ne « judiciariser » les renseignements obtenus ni trop en amont, à un stade où l'autorité judiciaire ne dispose pas de suffisamment d'éléments pour se saisir ou pour poursuivre utilement les investigations, ni trop en aval, à un stade où la légalité de la mise en œuvre de techniques de renseignement serait en cause.

Malgré des pratiques différentes selon les services et la difficulté à tracer une frontière précise entre le périmètre de la surveillance administrative et celui des procédures judiciaires, la commission s'attache à établir une doctrine cohérente dans un souci de prévisibilité de ses avis et de respect du principe de séparation des pouvoirs. Elle peut ainsi inviter les services de renseignement à se rapprocher de l'autorité judiciaire compétente afin que celle-ci envisage de se saisir des faits pour lesquels l'octroi d'une technique de renseignement est demandé, dès lors qu'au regard des éléments

présentés au soutien de cette demande, les conditions d'une telle saisine apparaissent réunies. Elle peut être conduite à rendre des avis favorables « pour judiciariser », assortis d'un bref délai, lorsque les éléments recueillis par le service, sans encore caractériser formellement une infraction, permettent d'envisager une saisine de l'autorité judiciaire à brève échéance.

L'activité de contrôle *a posteriori* de la commission a également mis en lumière, au travers des échanges intervenant dans ce cadre avec les services de renseignement, que les services étaient eux-mêmes dans le besoin d'une meilleure coordination avec l'autorité judiciaire. En effet, compte tenu du principe de primauté du judiciaire sur l'administratif, la mise en œuvre d'une technique spéciale d'enquête à l'encontre d'une personne dans le cadre d'une procédure judiciaire peut, en certaines hypothèses, conduire à l'interruption automatique d'une technique de renseignement mise en œuvre par un service de renseignement en application des dispositions du code de la sécurité intérieure sans que celui-ci en soit informé, ni n'ait connaissance du périmètre exact de la saisine de l'autorité judiciaire.

C'est aux fins de répondre à ces difficultés que le législateur a d'ailleurs instauré, par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, dite PATR, un cadre légal permettant des échanges entre les services de renseignement et l'autorité judiciaire, sans méconnaître les dispositions de l'article 11 du code de procédure pénale[31]. Il a ainsi prévu, à l'article 706-105-1 du code de procédurale pénale, que, dans certains domaines, tels que la cybercriminalité et la criminalité organisée de très grande complexité relevant de la Juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO)[32], le procureur de Paris peut communiquer des éléments contenus dans les procédures judiciaires relatifs à certaines infractions aux services de renseignement du premier cercle et à certains services du second cercle[33].

31. L'article 11 du code de procédure pénale dispose que : « *Sauf dans le cas où la loi en dispose autrement et sans préjudice des droits de la défense, la procédure au cours de l'enquête et de l'instruction est secrète. Toute personne qui concourt à cette procédure est tenue au secret professionnel dans les conditions et sous les peines prévues à l'article 434-7-2 du code pénal* ».

32. Voir l'article 706-75 du code de procédure pénale.

33. Des dispositions similaires préexistaient en matière de prévention du terrorisme, voir à cet égard l'article 706-25-2 du code de procédure pénale.

2.2.2.| Les perspectives pour favoriser ces échanges

Dans le cadre de son contrôle *a priori* comme de son contrôle *a posteriori*, la CNCTR doit s'assurer du respect du périmètre d'intervention de l'autorité judiciaire lorsque procédures judiciaire et administrative coexistent à l'encontre d'un même individu. À cette fin, il apparaît indispensable que la CNCTR soit rendue systématiquement destinataire de l'ensemble des éléments nécessaires lui permettant de rendre ses avis de manière éclairée.

Ces informations ne peuvent toutefois pas être obtenues directement auprès de l'autorité judiciaire. Bien que la commission rencontre régulièrement les procureurs de la République de certains tribunaux judiciaires dans le cadre de ses déplacements sur le territoire afin d'échanger sur les spécificités de la délinquance et de la criminalité locales, elle ne peut pas adresser de demande d'informations sur des cas précis. Les règles de préservation du secret de la défense nationale s'y opposent en effet.

Il est donc nécessaire que les services de renseignement apportent les informations indispensables au contrôle du respect de la compétence de l'autorité judiciaire dans la motivation de leurs demandes de technique de renseignement à la commission.

Cette préoccupation doit en outre permettre, *via* une communication renforcée avec l'autorité judiciaire, d'établir immédiatement si une menace distincte des faits dont elle est déjà saisie est caractérisée ou non.

Tableau synthétique des infractions entrant dans le champ de la « finalité 6 »

INFRACTIONS ENTRANT DANS LE CHAMP DE LA FINALITÉ 6 RÉGIME DE L'ARTICLE 706-73 CPP			
CLASSE EN CRIMINALITÉ ORGANISÉE PAR	**INFRACTIONS**	**EXIGENCE BANDE ORGANISÉE**	**TEXTES INCRIMINATEURS**
706-73, 1°	**Meurtre** en bande organisée	**OUI**	**Code pénal, art. 221-1 et 221-4 8°**
706-73, 2°	**Torture** ou **actes de barbarie** en bande organisée	**OUI**	**Code pénal, art. 222-1 et 222-4**
706-73, 2°bis	**Viol en concours** avec un ou plusieurs autres viols commis sur d'autres victimes	**NON**	**Code pénal, art. 222-23**
706-73, 3°	**Trafic de stupéfiants**	**NON**	**Code pénal, art. 222-34 à 222-40**
706-73, 4°	**Enlèvement** ou **séquestration**	**OUI**	**Code pénal, art. 224-1 et 224-5-2**
706-73, 5°	**Traite des êtres humains aggravée** par l'une des circonstances aggravantes prévues par les articles 225-4-2 à 225-4-4 du code pénal, parmi lesquelles la BO	**NON**	**Code pénal, art. 225-4-1 à 225-4-4**
706-73, 6°	**Proxénétisme aggravé** par l'une des circonstances aggravantes prévues par les articles 225-7 à 225-12 parmi lesquelles la commission en réunion, à l'égard de plusieurs victimes, à l'égard d'un mineur et la BO	**NON**	**Code pénal, art. 225-5 et 225-6** **Code pénal, art. 225-7 à 225-12**
706-73, 7°	**Vol** en bande organisée	**OUI**	**Code pénal, art. 311-9**
706-73, 8°	**Extorsion** criminelle prévue par les articles 312-6 ou 312-7 du code pénal : en bande organisée, **ou** avec actes de torture et de barbarie, **ou** avec violences ayant entraîné la mort	**NON** (voir autres circons-tances)	**Code pénal, art. 312-1, al1** **Code pénal, art. 312-6 et 312-7**
706-73, 9°	**Destruction, dégradation ou détérioration du bien d'autrui par substance explosive, incendie ou moyen dangereux pour les personnes** en bande organisée	**OUI**	**Code pénal, art. 322-6 et 322-8**
706-73, 10°	**Faux monnayage (fabrication)** : contrefaçon, falsification ou fabrication irrégulière de pièces de monnaie ou billets de banque	**NON**	**Code pénal, art. 442-1**
706-73, 10°	**Faux monnayage (mise en circulation)** : transport, mise en circulation ou détention en vue de la mise en circulation de pièces de monnaie ou billets de banque contrefaits, falsifiés ou fabriqués irrégulièrement	**OUI**	**Code pénal, art. 442-2**

INFRACTIONS ENTRANT DANS LE CHAMP DE LA FINALITÉ 6 RÉGIME DE L'ARTICLE 706-73 CPP			
CLASSE EN CRIMINALITÉ ORGANISÉE PAR	**INFRACTIONS**	**EXIGENCE BANDE ORGANISÉE**	**TEXTES INCRIMINATEURS**
706-73, 12°	**Armes et munitions (trafic)** : acquisition, détention, cession illicites, port ou transport illicites, hors du domicile, de matériels de guerre, armes, éléments d'armes ou munitions des catégories A ou B. Détention d'un dépôt d'armes ou munitions des catégories A et B. Importation illicite d'armes de guerre, ou d'armes ou munitions de catégorie A, B, C et de certaines armes de catégorie D	**NON**	**Code pénal, art. 222-52** **Code pénal, art. 222-53** **Code pénal, art. 222-54** **Code de la défense nationale, art. L. 2339-10**
706-73, 12°	**Armes et munitions (matériel de guerre)** : fabrication ou commerce illicite de matériel de guerre	-	**Code de la défense nationale, art. L. 2339-2**
706-73, 12°	**Armes et munitions (fabrication)** : constitution ou reconstitution d'une arme, ou modification d'une arme ayant pour effet d'en changer la catégorie	**NON**	**Code pénal, art. 222-59**
706-73, 12°	**Armes et munitions (produit explosif)** : détention ou transport de substances ou produits incendiaires ou explosifs, ou d'éléments entrant dans leur composition, en vue de la préparation, de la dégradation ou de la détérioration d'un bien ou d'atteintes aux personnes	**NON**	**Code pénal, art. 322-1-1**
706-73, 12°	**Armes et munitions (produit explosif)** : fabrication illicite d'engin explosif ou incendiaire, de produit explosif, ou d'élément ou substance destinés à entrer dans la composition d'un produit explosif	**NON**	**Code de la défense nationale, art. L. 2353-4**
706-73, 13°	**Aide à l'entrée, à la circulation et au séjour irrégulier d'un étranger** en France en bande organisée	**OUI**	**Code de l'entrée et du séjour des étrangers et du droit d'asile, art. L. 823-1 et L. 823-2**
706-73, 14°	**Blanchiment** ou **recel** du produit, des revenus ou des choses provenant d'une infraction mentionnée aux 1° à 13° de l'article 706-73 (*soit les infractions reportées ci-dessus*).	**NON**	**Code pénal, art. 324-1 et 324-2** **Code pénal, art. 321-1 et 321-2**
706-73, 15°	**Association de malfaiteurs** ayant pour objet la préparation d'une des infraction mentionnées aux 1° à 14° de l'article 706-73 (*soit les infractions reportées ci-dessus*).	**NON**	**Code pénal, art. 450-1**
706-73, 17°	**Détournement d'aéronef, de navire ou de tout autre moyen de transport** en bande organisée	**OUI**	**Code pénal, art. 224-6 et 224-6-1**

INFRACTIONS ENTRANT DANS LE CHAMP DE LA FINALITÉ 6 RÉGIME DE L'ARTICLE 706-73 CPP			
CLASSE EN CRIMINALITÉ ORGANISÉE PAR	**INFRACTIONS**	**EXIGENCE BANDE ORGANISÉE**	**TEXTES INCRIMINATEURS**
706-73, 16°	**Non justification de ressources** correspondant au train de vie en relation avec l'une des infractions mentionnées aux 1° à 15° et 17° de l'article 706-73 (*soit les infractions reportées ci-dessus*)	**NON**	**Code pénal, art. 321-6 et 321-6-1**
706-73, 19°	**Environnement** : exploitation d'une mine ou disposition d'une substance concessible, sans titre d'exploitation ni autorisation, avec atteinte à l'environnement, en bande organisée et connexe avec l'une des infractions mentionnées aux 1° à 17° de l'article 706-73	**OUI**	**Code minier, art. L. 512-2**
706-73, 20°	**Abus de faiblesse** en bande organisée	**OUI**	**Code pénal, art. 223-15-2**
706-73, 21°	**Infractions douanières** : contrebande, importation ou exportation sans déclaration de marchandises dangereuses pour la santé, la moralité ou la sécurité publiques, dont la liste est fixée par arrêté du ministre chargé des douanes, ou commis en bande organisée	**NON**	**Code des douanes, art. 414, al.3**

INFRACTIONS ENTRANT DANS LE CHAMP DE LA FINALITE 6 REGIME DE L'ARTICLE 706-73-1 CPP			
CLASSE EN CRIMINALITÉ ORGANISÉE PAR	**INFRACTIONS**	**EXIGENCE BANDE ORGANISÉE**	**TEXTES INCRIMINATEURS**
706-73-1, 1°	**Escroquerie** en bande organisée	**OUI**	**Code pénal, art. 313-1 et 313-2**
706-73-1, 1°	**Atteinte à un système de traitement automatisé de données** en bande organisée	**OUI**	**Code pénal, art. 323-1, 323-3-1** **Code pénal, art. 323-4-1**
706-73-1, 1°	**Évasion** en bande organisée	**OUI**	**Code pénal, art. 434-27 et 434-29, 1°** **Code pénal, art. 434-30, al 2**
706-73-1, 2°	**Travail dissimulé** en bande organisée	**OUI**	**Code du travail, art. L. 8221-1, 1° et 3°**
706-73-1, 3°	**Recel** du produit, des revenus ou des choses provenant d'une infraction mentionnée aux 1° et 2° de l'article 706-73-1 (*soit les infractions reportées ci-dessus*).	**NON**	**Code pénal, art. 321-1 et 321-2**
706-73-1, 3°	**Blanchiment** du produit, des revenus ou des choses provenant d'une infraction mentionnée aux 1° et 2° de l'article 706-73-1 (*soit les infractions reportées ci-dessus*).	**NON**	**Code pénal, art. 324-1**
706-73-1, 3° *bis*	**Blanchiment** en bande organisée de toute autre infraction que celles visées au 14° de l'article 706-73 (*voir tableau*)	**OUI** (ou à titre habituel ou facilité par l'activité profession-nelle)	**Code pénal, art. 324-2**
706-73-1, 4°	**Association de malfaiteurs** ayant pour objet la préparation d'une des infraction mentionnées aux 1° à 3° de l'article 706-73-1 (*soit les infractions reportées ci-dessus*).	**NON**	**Code pénal, art. 450-1**
706-73-1, 5°	**Non justification de ressources** correspondant au train de vie en relation avec l'une des infractions mentionnées aux 1° à 4° de l'article 706-73-1 (*soit les infractions reportées ci-dessus*)	**NON**	**Code pénal, art. 321-6 et 321-6-1**

INFRACTIONS ENTRANT DANS LE CHAMP DE LA FINALITE 6 REGIME DE L'ARTICLE 706-73-1 CPP			
CLASSE EN CRIMINALITÉ ORGANISÉE PAR	**INFRACTIONS**	**EXIGENCE BANDE ORGANISÉE**	**TEXTES INCRIMINATEURS**
706-73-1, 6°	**Trafic de biens culturels** soustraits sur un théâtre d'opérations terroristes	**NON**	**Code pénal, art. 322-3-2**
706-73-1, 7°	**Atteintes au patrimoine naturel** en bande organisée (espèces animales non domestiques, espèces végétales non cultivées, habitats naturels, sites d'intérêt géologique…)	**OUI**	**Code de l'environnement, art. L. 415-3 et L. 415-6**
706-73, 8°	**Trafic de produits phytopharmaceutiques** en bande organisée	**OUI**	**Code rural et de la pêche maritime, art. L. 253-15, L. 253-16, L. 253-17-1, 3° et L. 254-12, III**
706-73, 9°	**Délits relatifs aux déchets** en bande organisée	**OUI**	**Code de l'environnement, art. L. 541-46, I et VII**
706-73, 10°	**Jeux d'argent et de hasard** : participation à la tenue d'une maison de jeux d'argent et de hasard commis en bande organisée	**OUI**	**Code de la sécurité intérieure, art. L. 324-1, al 1**
706-73, 10°	**Jeux d'argent et de hasard** : importation, fabrication, détention, mise à disposition de tiers, d'installation et d'exploitation d'appareil de jeux d'argent et de hasard ou d'adresse commis en bande organisée	**OUI**	**Code de la sécurité intérieure, art. L. 324-4, al 1**
706-73, 13°	**Fraude sociale** : mise à disposition d'instruments de facilitation de la fraude sociale en bande organisée	**OUI**	**Code de la sécurité sociale, art. L. 114-13**

Étude 2. Surveiller l'entourage ?

Dans le langage courant, l'entourage correspond à l'« *ensemble de ceux qui entourent ordinairement quelqu'un, qui vivent dans sa familiarité* »[1].

Dans le code de la sécurité intérieure, où la notion est mentionnée aux articles L. 851-2 et L. 852-1[2], son acception est plus restreinte. Si le législateur ne l'a pas définie, il en a déterminé les contours en établissant son régime. Ainsi, l'entourage, au sens du code de la sécurité intérieure, correspond à l'ensemble de ceux à l'égard desquels certaines techniques de renseignement peuvent être mises en œuvre car ils « *sont susceptibles de fournir des informations au titre de la finalité* », du fait de leur proximité avec une cible elle-même en lien direct et personnel avec l'une des finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure[3].

La possibilité de surveiller les membres de l'entourage d'une cible a été introduite en droit positif par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

Si elle ne remet pas en cause le principe du caractère individualisé des techniques de renseignement (1), elle constitue toutefois une dérogation à ce principe selon lequel une personne ne peut faire l'objet d'une surveillance technique que si elle apparaît personnellement en lien avec une menace à conjurer ou un intérêt à protéger (2).

1. Dictionnaire de l'Académie française.

2. Le I de l'article L. 851-2 du code de la sécurité intérieure, relatif à l'accès aux données de connexion en temps réel, dispose ainsi notamment que « *(…) Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.* » Le I de l'article L. 852-1 du code de la sécurité intérieure, relatif aux interceptions de sécurité prévoit dans des termes quasiment identiques que : « *Lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes appartenant à l'entourage d'une personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée pour ces personnes* ».

3. L'article L. 811-3 énumère sept finalités permettant de justifier le recours aux techniques de renseignement prévues par le code de la sécurité intérieure soit : 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 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 ; 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; 4° La prévention du terrorisme ; 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 ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive.

1. Une dérogation au principe selon lequel les techniques de renseignement ne permettent de surveiller qu'une personne en lien direct avec une menace

Le cadre juridique antérieur à la loi du 24 juillet 2015[4] ne comportait pas de base légale expresse pour la mise en œuvre d'une surveillance technique à l'égard d'une personne faisant partie de l'entourage d'une cible (1.1). L'introduction d'une telle possibilité par la loi du 24 juillet 2015 n'a pas remis en cause l'exigence d'individualisation des surveillances techniques, le principe demeurant l'interdiction du suivi des proches d'une cible dès lors qu'ils ne font pas, eux-mêmes, l'objet d'une autorisation (1.2).

1.1. L'exigence d'une implication directe et personnelle des personnes susceptibles de faire l'objet de techniques de renseignement avant la loi du 24 juillet 2015

1.1.1. La loi du 10 juillet 1991 était silencieuse quant à la possibilité de mettre en œuvre des techniques de renseignement à l'égard des personnes qui, sans représenter par elles-mêmes une menace, étaient susceptibles de détenir des informations intéressantes en raison de leur présence dans l'entourage d'une cible.

L'ancien article L. 241-2 du code de la sécurité intérieure se bornait à prévoir que pouvaient « *être autorisées, à titre exceptionnel, dans*

4. Voir la loi n° 91946 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

les conditions prévues par l'article L. 242-1, les interceptions de correspondances émises par voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1 ».

En l'absence de base légale et malgré l'absence d'interdiction explicite de la loi, la commission nationale de contrôle des interceptions de sécurité (CNCIS) s'opposait à ce qu'une autorisation d'interception permette d'écouter les « *entourages d'une cible […] du seul fait de cette qualité* ». Chaque demande d'interception de sécurité était ainsi examinée à la lumière d'une exigence de « *présomption d'implication directe et personnelle* », la CNCIS vérifiant que la personne visée était « *bien l'auteur potentiel d'une infraction en préparation ou de l'acte mettant en cause divers intérêts nationaux* »[5].

1.1.2. Lors de l'examen de la loi du 24 juillet 2015 relative au renseignement, il est toutefois apparu que l'impossibilité de surveiller l'entourage de cibles limitait fortement la capacité des services de renseignement à prévenir certaines menaces.

L'évolution de la menace, notamment terroriste, a tout d'abord mis en lumière l'intérêt majeur des informations susceptibles d'être détenues par l'entourage des personnes identifiées comme porteuses d'une menace. Celles-ci communiquent en effet par différents moyens avec leur entourage qui, sans être lui-même impliqué dans quelque projet violent, détient potentiellement des informations d'intérêt relatives à leurs activités,

5. Voir 23ème rapport d'activité de la CNCIS, années 2014-2015, p. 21 : « *Il appartient à la Commission de vérifier que la personne visée est bien l'auteur potentiel de l'infraction en projet ou de l'acte mettant en cause divers intérêts nationaux. (…). La loi n'a jamais prévu qu'on puisse écouter « les entourages » (s'ils ne sont pas complices) du seul fait de cette qualité ; elle n'a pas davantage autorisé qu'on intercepte les communications des victimes* ».

leur localisation ou leurs contacts. Les membres de l'entourage constituent même parfois le seul canal de recueil de renseignement possible, notamment lorsque la cible principale ne peut être atteinte par des techniques de renseignement[6] (par exemple parce qu'elle n'est pas localisée ou qu'elle se trouve à l'étranger).

Il est par ailleurs apparu que si l'exigence d'une présomption d'implication directe et personnelle s'accordait bien à la recherche de renseignements utiles à la prévention de menaces susceptibles de recevoir une qualification pénale, elle était intellectuellement moins appropriée lorsque sont en cause des enjeux de prévention des atteintes aux intérêts fondamentaux de la Nation, plus éloignés du champ infractionnel.

En effet, dans ces domaines, par exemple en matière de protection des intérêts économiques de la Nation, la finalité de la surveillance est de rechercher des informations pertinentes qu'une personne est susceptible de détenir du seul fait de sa qualité ou de sa position. Cette dernière n'est alors pas soupçonnée d'agir comme auteur potentiel d'une infraction en préparation, mais uniquement identifiée comme détenant ou susceptible de détenir du renseignement pertinent[7].

L'évolution de la menace et la nécessité, pour la prévenir de façon efficace, de s'intéresser plus aux renseignements pertinents détenus par certaines personnes qu'à leur implication personnelle ont conduit le législateur en 2015 à permettre qu'une technique de renseignement soit mise en œuvre à l'égard de personnes faisant partie de l'entourage des cibles principales. Le principe demeure toutefois celui d'une surveillance individualisée qui interdit qu'une technique autorisée à l'encontre d'une personne conduise à la surveillance de personnes se trouvant dans son entourage en l'absence d'autorisation en ce sens.

6. Voir l'avis de la Commission nationale de l'informatique et des libertés (CNIL) du 4 mars 2015 sur le projet de loi relatif au renseignement, l'étude d'impact du 18 mars 2015 sur le projet de loi relatif au renseignement, et le rapport n° 2697 fait au nom de la commission des lois sur le projet de loi relatif au renseignement par M. Jean-Jacques Urvoas, enregistré à la présidence de l'Assemblée nationale le 2 avril 2015.

7. Ainsi, les surveillances tendant à la lutte contre les activités relevant de la criminalité ou de la délinquance organisée, ou encore à la prévention des comportements violents portent-elles naturellement sur des individus qui sont soupçonnés d'une implication coupable dans des faits, en préparation, qualifiables pénalement. « L'implication directe et personnelle » s'entend alors des éléments qui permettent de soupçonner que l'individu est bien susceptible de participer à l'un ou l'autre des éléments constitutifs d'un délit ou d'un crime en préparation. Cette exigence d'une implication « coupable » n'est en revanche pas pertinente lorsque la finalité poursuivie est la recherche de renseignements intéressant des domaines tels que la politique étrangère ou les intérêts économiques, industriels ou scientifiques majeurs de la France.

1.2. Un principe d'individualisation des surveillances qui demeure depuis 2015 et interdit les surveillances « collatérales »

La loi du 24 juillet 2015 a maintenu le principe du caractère individuel de la surveillance. L'article L. 8212 du code de la sécurité intérieure issu de cette loi dispose en effet que, lorsqu'un service de renseignement présente une demande de technique de renseignement, il doit notamment préciser : « *3° La ou les finalités poursuivies ; 4° Le ou les motifs des mesures ; […] 6° La ou les personnes, le ou les lieux ou véhicules concernés, […] les personnes dont l'identité n'est pas connue* [pouvant] *être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules* [pouvant] *être désignés par référence aux personnes faisant l'objet de la demande* ».

Si la loi prévoit désormais que des personnes faisant partie de l'entourage de cibles peuvent faire l'objet d'une surveillance technique en leur nom, ce n'est que sous certaines conditions précisément déterminées (voir ci-dessous). En dehors de ces situations et en l'absence d'autorisation accordée spécifiquement « *au titre de l'entourage* », la CNCTR veille à ce que la surveillance d'une cible ne conduise pas à celle de son entourage (1.2.1). Son contrôle est renforcé lorsque l'entourage d'une cible visée par une demande de technique de renseignement exerce une profession protégée (1.2.2).

1.2.1. Le contrôle des surveillances « collatérales » des entourages

La CNCTR veille à ce que les techniques autorisées ne portent pas une atteinte trop importante aux droits des tiers présents dans l'entourage d'une cible.

Dans le cadre de son contrôle *a priori* de proportionnalité, elle vérifie systématiquement que la nature et l'ampleur de l'atteinte à la vie privée des personnes se trouvant au contact ou à proximité de la cible principale, qui est susceptible de découler de la mise en œuvre d'une technique à son égard, notamment dans l'hypothèse de captation de son ou d'images, sont proportionnées à la réalité et à la gravité de la menace représentée par cette cible.

Dans le cadre de son contrôle *a posteriori*, la commission vérifie que le renseignement finalement conservé par le service a bien été recueilli alors que la cible principale était présente et qu'il est pertinent au titre de la prévention de la menace représentée par cette dernière. S'agissant des techniques dont l'exécution est centralisée, en particulier les interceptions de sécurité, le groupement interministériel de contrôle (GIC), qui est chargé de cette centralisation, procède lui-même à un contrôle systématique des communications captées et des retranscriptions réalisées afin de vérifier que la ligne écoutée est effectivement utilisée par la cible visée dans la demande et que les renseignements exploités portent bien sur cette dernière et non sur son interlocuteur, des membres de son entourage ou un autre utilisateur du sélecteur intercepté.

1.2.2. Le contrôle destiné à éviter une surveillances « détournée » des personnes qui exercent un mandat ou une profession protégée par le biais de leur entourage

Lorsqu'une personne surveillée a, dans son entourage une ou des personnes qui exercent une profession protégée au sens du code de la sécurité intérieure[8], la CNCTR vérifie que la surveillance n'a pas

8. L'article L. 821-7 du code de la sécurité intérieure interdit qu'un parlementaire, un magistrat, un avocat ou un journaliste puisse faire l'objet d'une technique de recueil de renseignement à raison de l'exercice de son mandat ou de sa profession. L'article L. 854-3 prévoit par ailleurs que : « *Les personnes qui exercent en France un mandat ou une profession mentionné à l'article L. 821-7 ne peuvent faire l'objet d'une surveillance individuelle de leurs communications à raison de l'exercice du mandat ou de la profession concerné* ». Voir le rapport d'activité 2022 de la CNCTR, p. 93 et suivantes.

pour objet ou pour conséquence de conduire à investiguer sur l'activité professionnelle protégée. Elle veille ainsi à ce qu'un service de renseignement ne puisse pas déployer une technique de renseignement à l'égard d'une personne faisant partie de l'entourage d'une personne exerçant un mandat ou une profession protégée dans le but d'accéder à des informations liées à l'activité protégée.

S'agissant par exemple du proche collaborateur d'un avocat ou d'un parlementaire, la commission fait en sorte que la surveillance de ce collaborateur soit bien « détachable » de l'activité de l'avocat ou de l'exercice du mandat du parlementaire[9]. Dans le cadre de son contrôle *a posteriori*, elle procède par ailleurs à une vérification systématique des productions recueillies par le service.

Le principe d'une surveillance individuelle demeure donc. Si l'entourage d'une cible peut, désormais, faire l'objet d'une surveillance technique, les services de renseignement doivent, pour ce faire, obtenir une autorisation spécifique.

9. Dans le cadre de son contrôle *a priori*, la CNCTR examine en conséquence la demande de surveillance technique en formation plénière. L'article L. 821-7 du code de la sécurité intérieure prévoit en effet *que « Lorsqu'une telle demande [de mise en œuvre d'une technique de recueil de renseignement] concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle des techniques de renseignement est examiné en formation plénière »* qui correspond à la composition la plus solennelle de la commission qui comprend l'ensemble des membres mentionnés à l'article L. 831-1 du code de la sécurité intérieure en vertu de son article L. 831-2 et qui ne peut valablement délibérer que si au moins quatre des neuf membres sont présents en vertu de l'article L. 832-3.

2. La possibilité d'une surveillance de l'entourage strictement encadrée

La surveillance de l'entourage de cibles ne s'envisage que dans le cadre d'un régime d'autorisation établi par la loi (2.1) et d'une définition des contours de la notion d'entourage élaborée par la CNCTR afin d'éviter toute surveillance non strictement nécessaire (2.2).

2.1. L'instauration progressive et limitée d'une surveillance technique de l'entourage

L'article L. 852-1 du code de la sécurité intérieure, créé par la loi du 24 juillet 2015 relative au renseignement, prévoit désormais que l'entourage d'une personne surveillée peut faire l'objet d'une interception de sécurité (2.1.1). Cette possibilité a, depuis, été étendue à des techniques moins intrusives (2.1.2).

2.1.1. L'ouverture de la surveillance de l'entourage aux interceptions de sécurité

L'article L. 852-1 du code de la sécurité intérieure prévoit la possibilité de mettre en œuvre une interception de sécurité à l'égard d'une personne faisant partie de l'entourage d'une cible : « *Lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes appartenant à l'entourage d'une personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée pour ces personnes* ».

Cette formulation résulte de débats nourris lors des travaux parlementaires au cours desquels des craintes quant à l'émergence d'une surveillance généralisée ont été émises. Lors des débats à l'Assemblée nationale, a ainsi été expressément ajoutée une exigence relative au sérieux des indices permettant de fonder la surveillance[10]. L'objectif est ainsi de limiter le nombre d'individus susceptibles d'être visés au titre de l'entourage, alors que le texte initial visait, non seulement les détenteurs d'informations d'intérêt, mais également les personnes susceptibles de jouer un rôle d'intermédiaire, de façon volontaire ou non. Cette notion d'« *intermédiaire involontaire* », qui était notamment censée viser le cas d'une personne dont les moyens de communication sont utilisés par la cible principale, même à son insu, a finalement été jugée trop imprécise lors des débats au Sénat avec le risque d'une atteinte portée à l'intimité de la vie privée d'un nombre potentiellement trop important de personnes. La reformulation retenue avait pour objectif de ne permettre la surveillance d'une personne de l'entourage d'une cible que « *pour autant qu'elle puisse fournir des informations relatives à la finalité poursuivie* » [11].

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a admis la conformité à la Constitution de cette possibilité de mettre en œuvre des interceptions de sécurité à l'égard de l'entourage d'une cible, en considérant que le législateur n'avait pas « *opéré une conciliation manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée et le secret des correspondances* »[12]. Parmi les garanties apportées par le législateur, le Conseil constitutionnel a notamment relevé que l'exécution des interceptions de sécurité était « *centralisée* », ce qui permettait un contrôle facilité de la CNCTR, et que le nombre d'interceptions de sécurité simultanément mises en œuvre était contingenté.

10. Voir l'amendement n° 44 du 7 avril 2015, présenté par M. CORONADO et autres, adopté lors des débats en séance publique à l'Assemblée Nationale qui a conduit à la rédaction intermédiaire : « *Lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes appartenant à l'entourage d'une personne concernée par l'autorisation sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour le compte de cette dernière ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation, celle-ci peut être accordée également pour ces personnes* ».

11. Voir l'amendement n° COM-75 du rapporteur de la commission des lois du Sénat, M. Philippe BAS.

12. Voir la décision n° 2015-173 DC du 23 juillet 2015, considérants 64 et s.

2.1.2. L'élargissement encadré de la surveillance de l'entourage à d'autres techniques moins intrusives

Porté par des considérations similaires à celles qui avaient prévalu lors des débats relatifs à la loi du 24 juillet 2015, le législateur a ouvert l'accès en temps réel aux données techniques de connexion de l'entourage par la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste dans les termes suivants : « *Lorsqu'il existe des raisons impérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes* »[13].

Cette disposition rédigée dans des termes très similaires à ceux retenus pour les interceptions de sécurité, a été déclarée contraire à la Constitution par le Conseil constitutionnel. En effet, saisi d'une question prioritaire de constitutionnalité visant les dispositions de l'article L. 851-2 du code de la sécurité intérieure, le Conseil constitutionnel a censuré l'absence de limitation du nombre d'autorisations susceptibles d'être simultanément en vigueur. Dans sa décision n° 2017-648 QPC du 4 août 2017, il a ainsi considéré qu'en permettant « *que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit* » et « *faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité* », « *le législateur n'[avait] pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée* »[14].

13. Voir l'article L. 851-2 du code de la sécurité intérieure.

14. Voir la décision n° 2017-648 QPC du 4 août 2017, considérant 11.

Pour se conformer aux exigences du Conseil constitutionnel, le législateur, par la loi n° 20171510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, a fait le choix de rétablir le dispositif prévu par la loi du 21 juillet 2016 en instaurant un nombre maximal d'autorisations pouvant être en vigueur simultanément s'agissant de la technique d'accès en temps réel aux données de connexion[15]. Les « raisons impérieuses » retenues par la loi du 21 juillet 2016 sont toutefois redevenues à cette occasion des « raisons sérieuses » de penser que la surveillance de l'entourage est susceptible de fournir des informations au titre de la finalité.

Par ailleurs, l'autorisation d'intercepter les communications d'une personne valant autorisation d'accéder à ses données de connexion en temps différé[16], la CNCTR admet que certaines de ces données puissent également faire l'objet d'autorisations d'accès à l'égard des personnes faisant partie de l'entourage des cibles. En effet, certaines données de connexion qui permettent de connaître l'identité des personnes faisant partie de l'entourage d'une cible, voire leurs propres contacts, sont en réalité recueillies dans le but de surveiller la cible principale en permettant de cartographier son relationnel.

La commission admet enfin qu'une personne se trouvant dans l'entourage d'une cible puisse faire l'objet d'une autorisation d'exploitation de ses communications internationales, cette technique pouvant être assimilée à une interception de sécurité dans le cadre des mesures de surveillance des communications électroniques internationales prévues aux articles L. 854-1 et suivants du code de la sécurité intérieure. Une telle autorisation est, en outre, soumise au même contrôle de la CNCTR et au respect d'un nombre maximal d'autorisations simultanément en vigueur[17], garanties procédurales jugées suffisantes par le Conseil constitutionnel dans ses décisions précitées pour permettre la surveillance de l'entourage.

15. Voir l'article 8 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.
16. En vertu des dispositions du III de l'article L. 852-1 du code de la sécurité intérieure.
17. Voir le V de l'article L. 854-2 du code de la sécurité intérieure.

Ce contingentement des autorisations permet de caractériser « *le lien étroit* » exigé par le Conseil constitutionnel dans sa décision du 4 août 2017 précitée entre les personnes susceptibles de faire l'objet d'une technique de renseignement et une menace, et constitue à cet égard un « *puissant facteur de régulation* » selon les termes employés par le rapporteur public du Conseil d'État dans ses conclusions relatives à l'affaire dite *French Data Network*[18].

C'est d'une part par le contrôle de l'existence de ce lien étroit entre la personne susceptible de faire l'objet d'une technique de renseignement au titre de l'entourage et une menace, d'autre part, par l'élaboration d'une doctrine visant à préciser les contours de cette notion d'entourage que la CNCTR s'attache à préserver l'équilibre entre l'objectif de prévention des atteintes aux intérêts de la Nation et le droit au respect de la vie privée. À cet égard, à l'occasion des débats relatifs à la loi du 30 octobre 2017 précitée, la commission des lois de l'Assemblée nationale avait retenu que : « *il appartiendra au Premier ministre, après avis de la CNCTR, de s'assurer que la personne concernée par la demande de recueil appartient bien à l'entourage d'une personne préalablement identifiée comme représentant une menace au regard de la nature des liens, de leur intensité, de leur régularité et de tout autre élément de nature à justifier le bien-fondé de la mesure* »[19].

2.2. La détermination progressive des contours de la notion d'entourage

Si la cible principale ne doit pas nécessairement faire l'objet de techniques de surveillance strictement identiques à celle envisagées

18. Voir conclusions de M. Alexandre LALLET, maître des requêtes du Conseil d'État, rapporteur public, sur les décisions CE, 21 avril 2021, *French Data Network et autres*, n° 393099 – *La Quadrature du Net et autres*, n° s 394922, 397851– *Association Igwan. net*, n° 397844– *Société Free mobile*, n° 424717 - *Société Free*, n° 424718, retenant que : « *Le contingentement des autorisations que le Conseil [constitutionnel] a estimé indispensable pour assurer le respect de la Constitution, constitue un puissant facteur de régulation à cet égard. A partir du moment où ce lien étroit est caractérisé, on peut considérer qu'il y une forme d'implication au sens où l'entend la Cour [de justice de l'Union européenne].* »

19. Rapport n° 164 de la commission des lois sur le projet de loi adopté par le Sénat renforçant la sécurité intérieure et la lutte contre le terrorisme (n° 104) par M. Raphaël GAUVAIN.

pour une personne appartenant à son entourage, la menace qu'elle porte doit être suffisamment identifiée et caractérisée (2.2.1). La CNCTR a également précisé le champ des personnes susceptibles d'être effectivement visées par une technique de renseignement « au titre de l'entourage » (2.2.2).

2.2.1. L'existence d'une cible principale constituant une menace suffisamment caractérisée, surveillée ou non

Face à une certaine ambiguïté des dispositions du code de la sécurité intérieure qui prévoient la possibilité de surveillance l'entourage d'une cible en mentionnant « *l'entourage d'une personne concernée par l'autorisation* »[20], la CNCTR, s'appuyant notamment sur le caractère individuel de la surveillance et sur le principe de subsidiarité, n'exige pas que la personne réellement ciblée fasse l'objet d'une technique de renseignement identique à celle sollicitée pour un membre de son entourage, ni même qu'elle fasse l'objet d'une quelconque technique.

Une autre interprétation des dispositions du code de la sécurité intérieure relatives à l'entourage aurait été susceptible d'aboutir à une situation paradoxale, au demeurant contraire à l'esprit de la loi tel qu'il résulte de l'examen des débats parlementaires. Elle aurait en effet conduit à considérer que lorsqu'une cible représente une menace telle que serait autorisée à son égard la mise en œuvre de techniques particulièrement intrusives telles qu'une sonorisation de son domicile ou le recueil de ses données informatiques, son entourage ne pourrait pas être visé par une autorisation d'interception de sécurité, alors même que cette technique de surveillance est moins intrusive, si la cible principale

20. Cette rédaction est issue d'un amendement n° CL 187 du 31 mars 2015 présenté par M. Jean-Jacques Urvoas, rapporteur de la commission des lois à l'Assemblée Nationale, modifiant la rédaction initiale qui faisait référence à l'entourage d'une personne « visée par l'autorisation ».

ne fait pas elle-même l'objet de cette technique. De même, la surveillance de proches d'une personne qui serait porteuse, depuis l'étranger, d'une menace caractérisée à l'encontre des intérêts fondamentaux de la Nation, ne serait pas possible dès lors que cette dernière, se trouvant en dehors du territoire national, n'est pas susceptible d'être visée par une technique de renseignement relevant de la surveillance domestique.

La réalité de la menace ne s'évalue donc pas uniquement à l'aune des techniques effectivement autorisées à l'égard de la cible principale. La CNCTR procède en la matière à une analyse au cas par cas de l'ensemble des éléments présentés par les services dans leurs motivations afin de vérifier que cette cible principale représente bien une menace.

La CNCTR veille, en effet, à ce que les services fassent état, dans leurs demandes, d'éléments suffisants en la matière. La cible principale doit ainsi être identifiée ou identifiable. Si son identité est inconnue, la demande doit détailler les éléments permettant de déterminer son implication personnelle au titre de la finalité qui justifie la mise en œuvre d'une surveillance technique. L'existence de techniques de renseignement mises en œuvre à l'égard de la cible principale demeure néanmoins un critère important d'appréciation.,

2.2.2. Une personne susceptible de détenir des informations en raison de sa présence dans l'entourage d'une cible

Le suivi technique de certaines personnes faisant partie de l'entourage d'une cible ne relève toutefois pas toujours d'une surveillance « au titre de l'entourage » au sens des dispositions du code de la sécurité intérieure.

En effet, les personnes faisant partie de l'entourage d'une cible sont, d'abord, susceptibles de faire l'objet d'un suivi au titre de leur implication personnelle. Ainsi, lorsque le service fait état d'éléments permettant de penser que la personne est soupçonnée d'apporter, en connaissance de cause, son assistance à la cible principale, l'autorisation est accordée au titre de l'implication personnelle de cette personne, qui plus qu'à un proche, peut être assimilée à un complice. L'ancrage d'une personne au sein d'un mouvement ou d'un groupe portant une atteinte avérée aux intérêts fondamentaux de la Nation peut également être tel qu'il permet de suffisamment caractériser qu'elle est en fait elle-même impliquée personnellement.

Dès lors que l'autorisation est accordée au titre de l'implication personnelle de la personne, la gamme des techniques de renseignement susceptibles d'être mises en œuvre s'élargit. La CNCTR ne procède toutefois pas à une requalification d'office d'une demande visant une personne au seul titre de l'entourage considérant, d'une part, que ce serait aller au-delà de cette demande, ce qui n'est pas la fonction de la commission, d'autre part, en pratique, que la surveillance d'une cible au titre de l'entourage ne représente en tout état de cause pas un obstacle à ce que le service recueille et exploite des éléments qui viendraient établir que la personne représente en réalité elle-même une menace.

Lorsqu'une personne faisant partie de l'entourage d'une cible n'est pas elle-même impliquée dans la menace identifiée, la CNCTR contrôle qu'elle est suffisamment proche de cette cible principale. Elle écarte ainsi les surveillances de « l'entourage indirect » d'une cible et exige que le service fasse état d'éléments suffisants permettant de déterminer la nature et l'intensité des liens qui unissent la cible principale à la personne faisant l'objet de la demande de surveillance technique « *au titre de l'entourage* ». Elle vérifie également le caractère actuel des liens avec cette cible

principale. Ainsi, les demandes faisant état de liens hypothétiques ou trop anciens font-elles *a minima* l'objet de demandes de renseignements complémentaires destinés à étayer l'intensité et l'actualité de ces liens et, le cas échéant, d'avis défavorables.

Au-delà, la CNCTR vérifie surtout que le service fait état, de façon suffisante, de l'existence d'indices sérieux permettant de penser que la cible détient des informations d'intérêt relatives à la cible principale. La détention d'informations d'intérêt constitue en effet l'élément de démonstration le plus important à caractériser. S'il est rempli, la CNCTR admet par exemple que la personne susceptible de détenir de telles informations en lien avec une cible d'intérêt ne soit pas identifiée par le service au moment où il formule sa demande.

Ces indices peuvent résulter des liens de proximité forts qu'entretiennent les deux personnes ou encore du fait que la personne identifiée comme faisant partie de l'entourage d'une cible est susceptible d'être détentrice de supports ou documents appartenant à cette dernière. Le service doit, en tout état de cause, désigner aussi précisément que possible les informations que la personne est susceptible de détenir, ainsi que leur lien avec la cible principale et la finalité poursuivie par la surveillance.

Éclairages

Éclairage 1. L'intelligence artificielle (IA) et le renseignement

Éclairage 2. L'usage responsable des capacités commerciales de cyber-intrusion : une perspective diplomatique

(Contribution de M. Henri VERDIER, ambassadeur pour le numérique et de M. Léonard ROLLAND, sous-directeur de la cyber-sécurité à la direction des affaires stratégiques, de sécurité et du désarmement au ministère de l'Europe et des affaires étrangères).

Éclairage 1. L'intelligence artificielle (IA) et le renseignement

« À l'instar de la machine à vapeur ou de l'électricité dans le passé, l'IA est en train de transformer notre monde, notre société et notre industrie (…) / Notre approche de l'IA définira le monde dans lequel nous vivons. ». C'est ainsi que la Commission européenne, dans sa communication du 25 avril 2018 sur l'intelligence artificielle (IA) pour l'Europe[1], introduisait les enjeux du développement d'une technologie présentée comme l'une des plus innovantes et stratégiques du XXIe siècle, au point d'en faire l'initiatrice d'une 4ème révolution industrielle.

Cinq ans plus tard, l'année 2023 s'est révélée particulièrement riche en actualités sur cette thématique, qui débute avec la découverte par le grand public du robot conversationnel ChatGPT[2] déployé en libre accès par l'entreprise californienne OpenAI, et se termine par l'annonce le 8 décembre d'un accord politique au sein de l'Union européenne[3] pour réguler l'utilisation de l'intelligence artificielle au moyen d'un règlement *ad hoc* (projet de règlement **établissant des règles harmonisées concernant l'intelligence artificielle ou** *Artificial Intelligence Act*, *AI Act*).

Le concept d'IA, né dans les années 1950 dans les milieux de la cybernétique[4] et longtemps relégué au champ de la science-fiction, n'a jamais été aussi présent dans le débat public, la succession d'annonces sur les avancées réalisées en la matière dans un nombre

1. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 25 avril 2018, *L'intelligence artificielle pour l'Europe*, COM (2018) 237 final.
2. Déploiement en libre accès fin novembre 2022 de Chat GPT (*Chat Generative Pre-trained Transformer* (version GPT3.5), technologie permettant la génération de texte de manière autonome par une intelligence artificielle.
3. Accord politique du Parlement européen et du Conseil sur le règlement concernant l'intelligence artificielle, proposé par la Commission en avril 2021.
4. L'officialisation du concept est généralement datée de la conférence organisée à l'été 1956 par John McCarthy et Marvin Minsky au Dartmouth College (New Hampshire, États-Unis). Peu avant, Alan Turing, regardé comme l'un des pères fondateurs de l'IA avec John Von Neumann, John McCarthy et Marvin Minsky, a publié en 1950 un article intitulé *Computing Machinery and Intelligence* questionnant de manière inédite la limite entre l'humain et la machine.

croissant de secteurs trouvant écho dans le foisonnement des réflexions et questionnements sur les enjeux éthiques et sociétaux soulevés.

La présente étude ne définit pas l'IA, ni même ne prétend choisir parmi les nombreuses définitions existantes qui peuvent renvoyer tant à une discipline scientifique, dont le but est de parvenir à faire imiter par une machine les capacités cognitives d'un être humain[5], qu'aux technologies concrètes qui sont issues de ce champ académique de recherche[6/7]. Dans une approche pragmatique, la présente introduction se borne à délimiter le champ de la réflexion engagée, qui porte sur les impacts et enjeux, dans le domaine du renseignement, de tout procédé automatisé qui, à partir de données reçues, génère des résultats tels que des contenus, des prévisions, des recommandations ou des décisions. Les systèmes retenus – appelés par commodité dans la suite du propos « système d'intelligence artificielle » ou « SIA » - englobent ainsi les traitements automatisés complexes de gestion des données et toutes les techniques d'algorithmes et de systèmes apprenants, à l'exclusion des systèmes logiciels et traitements simples et d'utilisation courante, qui ne soulèvent pas les mêmes difficultés.

5. En ce sens, la définition historique retenue par Marvin Minsky fait de l'intelligence artificielle la science qui consiste à faire faire à des machines ce que l'homme fait moyennant une certaine intelligence (voir notamment *The Society of Mind,* 1986). Voir aussi la définition retenue par la Commission d'enrichissement de la langue française dans le *Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptés),* publié au JORF n° 0285 du 9 décembre 2018 : « *Champ interdisciplinaire théorique et pratique qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel et logiciel, à des fins d'assistance ou de substitution à des activités humaines.* »

6. Pour le Parlement européen, l'intelligence artificielle désigne la « *possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité* ». (Site Internet : Intelligence artificielle : définition et utilisation).

7. Suivant la notion d' « intelligence » retenue, on distingue parfois l'IA dite « forte » et l'IA qualifiée de « faible » ou « modérée ». **Les systèmes d'IA « faibles » ou « modérés »** renvoient à des systèmes en mesure d'exécuter des tâches très complexes grâce à leur capacité de gestion de l'information. Ces systèmes s'appuient sur l'une des composantes de l'intelligence humaine, la puissance cognitive, pour réaliser les seules fonctions pour lesquelles elles ont été conçues, sans conscience, ni sensibilité. **L'IA « forte » ou « générale »** vise les machines qui seraient dotées d'une forme de conscience d'elles-mêmes et capable de réaliser de manière totalement autonome une infinité de tâches, imitant ainsi une cognition humaine. Elle relève aujourd'hui du domaine de la pure science-fiction ; en l'absence de rupture technologique majeure, les avancées scientifiques actuelles ne permettent pas d'envisager de doter une machine de l'ensemble des facultés humaines.

DES NOTIONS À DISTINGUER : SYSTÈME D'INTELLIGENCE ARTIFICIELLE (SIA) ET ALGORITHME, SYSTÈME EXPERT ET SYSTÈME APPRENANT

Dans le débat public actuel, l'IA est souvent assimilée à une catégorie particulière d'algorithme, basé sur des techniques dites d'apprentissage. Les notions d'IA et d'algorithme doivent pourtant être distinguées, l'algorithme étant une technique servant à la construction des SIA. La plupart des SIA reposent sur un ou plusieurs algorithmes.

L'algorithme se définit usuellement comme une suite d'instructions précises permettant d'aboutir à un résultat à partir de données fournies en entrée.

Les algorithmes sont très divers. De manière schématique, ils peuvent se rattacher à deux grandes catégories conceptuelles de SIA, selon qu'ils relèvent de l'IA symbolique (ou cognitiviste) ou de l'IA connexionniste, soit l'un des deux grands courants apparus dès le commencement des travaux sur l'IA dans les années 1950.

L'**IA symbolique** relève d'une approche logique du traitement de l'information : tout problème à résoudre est décomposé en une succession d'actions logiques simples et programmées pour qu'une machine puisse les effectuer rapidement. Se rattachent à ce courant les SIA dits « systèmes experts », les programmes informatiques capables de résoudre des problèmes complexes par l'application de règles précises en utilisant une masse de connaissances pointues.

L'**IA connexionniste** se fonde, elle, sur une approche probabiliste du traitement de l'information, et vise à permettre « l'apprentissage » par la machine à partir d'une très grande masse de données. L'application la plus connue de ce courant est l'apprentissage automatique (ou « *machine learning* »), technique consistant à construire des algorithmes qui « apprennent » seuls, c'est-à-dire sont capables de modifier eux-mêmes leurs paramètres entraînables afin d'obtenir les meilleures performances. S'inscrivent aussi dans ce courant les systèmes dit d'intelligence artificielle « générative », capables de produire un contenu nouveau original à partir de données

ayant servi à leur apprentissage. La notion de « réseaux de neurones artificiels » est parfois utilisée pour décrire les SIA reposant sur une approche connexionniste, en particulier lorsqu'il est question d'« apprentissage profond » (« deep learning »), procédé d'apprentissage automatique possédant de très nombreux paramètres (plusieurs couches de réseaux neuronaux artificiels).

En pratique, la classification la plus usuelle retenue des procédés d'IA distingue les systèmes « **experts** » des systèmes « **apprenants** ».

Les SIA combinent fréquemment des algorithmes relevant de ces deux approches.

Ces dix dernières années ont ainsi été marquées par l'essor impressionnant des SIA grâce à l'accès à des volumes massifs de données permis par les technologies de l'information et de la communication, et au développement de la puissance de calcul des outils numériques. Au-delà des sentiments contrastés, enthousiasme ou inquiétude, que suscite toute révolution technique, les SIA sont des technologies du présent qui bouleversent d'ores et déjà le domaine du renseignement comme tous les secteurs d'activités, appelant une vigilance renforcée des autorités de régulation et de contrôle.

1. L'IA est déjà largement utilisée en matière de défense et de sécurité, dans un cadre juridique qui reste lacunaire

1.1. Le développement de l'usage des systèmes d'intelligence artificielle (SIA) en matière de défense et de sécurité

1.1.1. La multiplication des cas d'emploi en matière de défense et sécurité, notamment pour le renseignement

Le domaine de la sécurité et de la défense est un champ privilégié de recherche et d'application en matière d'IA. Les premiers développements historiques des technologies d'IA ont d'ailleurs porté sur le traitement automatisé des langues (TAL) à des fins de défense[8]. D'intenses recherches ont été menées au milieu du siècle dernier, en particulier aux États-Unis et en Angleterre, visant à la création de programmes de traduction automatique, principalement dans la paire de langues anglais-russe. Bénéficiant du soutien des autorités publiques américaines, ces recherches répondaient à un objectif de guerre afin de traduire les communications soviétiques captées.

8. Ce champ de recherche a été lancé à la suite des succès en matière de décryptage rencontrées pendant la seconde guerre mondiale et sous l'impulsion de Warren Waever. Ce pionnier du TAL a proposé d'utiliser des ordinateurs pour « décoder » ou « déchiffrer » le langage dans son célèbre mémorandum, *Translation,* publié en 1949. La démarche a pris son essor dès les années 50.

Aujourd'hui, au-delà de l'usage évident en matière d'administration des forces de défense et de sécurité (gestion du personnel, logistique, maintenance, etc.), les procédés d'intelligence artificielle sont très présents au plan opérationnel, dans la mise en œuvre même des activités de sécurité, sous leurs nombreuses formes (traitement automatisé de l'information, interfaces homme-machine, robotique, etc.).

Il n'existe pas de recensement exhaustif de tous les cas d'usage des SIA par les autorités publiques en charge des politiques de défense et de sécurité, mais quelques exemples de développements récents permettent d'illustrer l'utilité et l'importance de ces procédés[9].

Le domaine de la défense est sans doute celui où l'usage de l'IA est le plus ancien et le plus intense. Aujourd'hui, l'utilisation des SIA en cette matière est très importante pour la conduite opérationnelle, de l'appui au combat jusqu'aux systèmes d'armes, les matériels de combats les plus sophistiqués utilisant tous un ou plusieurs SIA.

En 2023, le recours possible à des « robots tueurs » a ainsi suscité de vifs débats sur la scène internationale eu égard au risque que représente la suppression du contrôle humain dans le recours à la force[10]. Sans aller jusqu'à cette possibilité d'utilisation d'un engin armé autonome sans tutelle humaine, les systèmes d'armes automatisés, possiblement létaux[11], existent depuis longtemps et la recherche pour développer l'autonomie des systèmes d'armes n'a fait que s'accélérer ces dernières années avec l'essor des méthodes d'apprentissage de l'IA (ou **«** *machine learning* »).

9. Voir notamment l'étude réalisée par le Conseil d'État à la demande du Premier ministre, *Intelligence artificielle et action publique : Construire la confiance, Servir la performance*, adoptée en assemblée générale plénière le 31 mars 2022, qui comporte une cartographie des cas d'usage de l'IA notamment dans les domaines de la défense et de la sécurité et des activités d'enquête, de contrôle et de sanction (annexe 9).

10. À cet égard, une résolution 78/241 de l'Assemblée générale des Nations-Unies, votée par 152 pays le 22 décembre 2023, relève que « *les enjeux de taille et les vives inquiétudes que soulève [...] l'utilisation de nouvelles applications technologiques dans le domaine militaire, y compris celles liées à l'intelligence artificielle et à l'autonomie des systèmes d'armes* », témoignant tant des développements techniques issus de l'IA que des enjeux entourant les nouvelles formes d'armes désignées sous le vocable de « *systèmes d'armes létaux autonomes* » (ou SALA).

11. Parmi ces systèmes d'armes létales automatisées, figurent par exemple les **systèmes de défense antimissile**, dont le succès technique repose sur l'IA, dès lors que le délai de réaction, pour pouvoir être utilement employés, exclut le recours à une décision humaine (autre que de principe en amont, en activant le système), ou encore, de façon plus récente, les **drones armés** tels que les drones *Predator* et *Reaper* de la société américaine *General Atomics Aeronautical Systems,* dont certains ont été ou sont utilisés dans des conflits, notamment au Moyen-Orient ou en Ukraine.

S'il paraît plus modeste au regard des usages ainsi développés en matière de défense, le déploiement de l'IA pour opérer des surveillances, publiques ou secrètes, s'est accéléré ces dernières années.

Ainsi, **s'agissant de la sécurité publique**, l'un des développements les plus remarqués porte sur la sécurisation de espaces publics au moyen de caméras dites « intelligentes » (ou « augmentées »), associant des dispositifs de captation d'images (appareils de vidéoprotection, caméras embarquées ou aéroportées, etc.) à des SIA analysant les flux de données qui en sont issus pour détecter des anomalies, des comportements ou activités suspects, ou des situations à risque.

La loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024[12] prévoit ainsi, à titre expérimental jusqu'au 31 mars 2025 et dans le cadre de manifestations sportives, récréatives ou culturelles d'ampleur, que les images collectées au moyen d'un système de vidéoprotection ou de caméras installées sur des aéronefs peuvent faire l'objet de traitements algorithmiques afin de détecter en temps réel et signaler certains événements prédéterminés présentant ou révélant des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes. Sont exclus de cette expérimentation les SIA les plus intrusifs, correspondant aux traitements algorithmiques recourant à des données biométriques[13/14].

Toutefois, si l'usage de SIA publics utilisant les données biométriques est pour l'heure prohibé, à l'exception des dispositifs d'authentification dans le cadre du traitement des antécédents judiciaires (TAJ) et du système de passage rapide aux frontières extérieures (Parafe)[15], des SIA

12. Voir l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.

13. Il s'agit des caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique.

14. Voir décision 2023-850 DC du 17 mai 2023 du Conseil constitutionnel, csdt 42.

15. Deux expérimentations ont par ailleurs été menées sur des dispositifs de vidéosurveillance avec reconnaissance faciale lors du carnaval de Nice en 2019 et lors d'un match de l'Olympique de Marseille en 2021.

permettant d'identifier les personnes physiques grâce à des procédés de reconnaissance biométrique, notamment faciale, qui ont connu de très importants progrès dans la période récente et sont largement répandus dans la sphère privée[16], connaissent déjà des usages importants en matière de sécurité et de préservation de l'ordre public dans nombre de pays (Chine et États-Unis notamment).

De même, **en matière d'enquêtes et de détection d'infractions,** les SIA sont utilisés de manière croissante pour permettre une remontée d'informations, grâce à l'exploitation massive des flux de données qu'ils autorisent.

À titre d'exemple, les services fiscaux expérimentent ainsi depuis 2021 un nouvel outil de collecte et d'exploitation de données publiquement disponibles en ligne, à des fins de détection de certaines infractions fiscales[17]. L'exploitation et le croisement de données (« *data mining* »[18]) rendus possibles par les technologies d'IA permet à la direction générale des finances publiques de repérer des profils de fraude en analysant et en recoupant, par le biais d'algorithmes, toutes les informations dont elle dispose.

QUELQUES NOTIONS À CONNAÎTRE

Data mining (ou fouille de données) : procédé consistant à rechercher et explorer automatiquement de grandes quantités de données afin de découvrir des tendances et des modèles qui vont au-delà de la simple analyse.

OSINT (ou renseignement de sources ouvertes) : acronyme d'Open Source Intelligence, cette notion renvoie, en matière de sécurité, à une méthode de collecte et d'analyse de renseignements à partir des informations et données en libre accès.

16. Par exemple aux fins d'authentification, comme pour les procédés d'identification des smartphones.

17. Voir l'article 154 de la loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020 et la prolongation de l'expérimentation jusqu'au 31 décembre 2026 fixée par l'article 112 de la loi n° 2023-1322 du 29 décembre 2023 de finances pour 2024.

18. Le « *data mining* » serait à l'origine de 52 % des contrôles fiscaux en 2022.

En matière de défense numérique, la surveillance de l'espace cyber s'est nettement renforcée ces dernières années, parallèlement au constat de l'importance prise par les réseaux sociaux dans le processus de fabrication et de diffusion de l'information et de la multiplication des opérations de manipulation de l'information menées par des organisations ou État étrangers. À cet égard, les autorités françaises ont créé en 2021 le service Viginum, dont la mission consiste à détecter et caractériser des ingérences numériques étrangères affectant le débat public numérique en France, notamment en période électorale. Pour opérer sa surveillance, ce service utilise des procédés algorithmiques permettant de collecter et traiter les données issues des contenus accessibles publiquement sur les plateformes en ligne sur lesquels il est autorisé à investiguer.

Les techniques de renseignement régies par le livre VIII du code de la sécurité intérieure, n'échappent pas au développement de l'usage des SIA tant au stade de la collecte de données qu'au stade de leur pré-exploitation ou de leur exploitation.

C'est essentiellement pour l'exploitation et l'analyse technique des données recueillies par les capteurs que l'usage des SIA s'est imposé, les volumétries concernées ne permettant plus que l'homme opère sans machine leur traitement exhaustif. Des technologies automatisées de gestion et de traitement des mégadonnées sont ainsi utilisées pour organiser et explorer les stocks de données, en assurer les prétraitements et en faciliter l'analyse. Les SIA constituent donc des procédés venant à l'appui de la mise en œuvre de certaines des techniques de renseignement prévues par le code de la sécurité intérieure.

EXEMPLES DE SIA UTILISÉS PAR LES SERVICES DE RENSEIGNEMENT

Logiciels « TAL » : les outils de traitement automatique du langage visent à analyser, interpréter et synthétiser du texte afin d'en extraire des connaissances sans intervention humaine, pour des applications très variée - de la traduction instantanée de conversations ou textes en une autre langue aux opérations de veille stratégique. Le groupe Systran, pionnier français et leader mondial des technologies de traduction automatique, est ainsi prestataire de plusieurs agences de renseignement.

Logiciels de Preligens : les logiciels de cette société, spécialisée en géo-intelligence, assurent le traitement et l'exploitation automatisés de grandes masses de données, en particulier satellitaires, au profit du renseignement interarmées français. Ils permettent, par exemple, de repérer des mouvements anormaux sur des sites sensibles, de détecter et décompter les engins de combats en zones de conflit, ou encore de cartographier des lieux inconnus.

Par ailleurs, sans que cette technique puisse être assimilée à un SIA, le code de la sécurité intérieure autorise le recours à des algorithmes « *pour les seuls besoins de la prévention du terrorisme* »[19]. Cette technique de renseignement, expérimentée à partir de 2015 puis pérennisée par la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement[20] vise à permettre la détection des menaces terroristes à partir de l'exploitation de données transitant par les réseaux des opérateurs de communications électroniques et des fournisseurs de services sur Internet. Les cinq algorithmes actuellement autorisés[21] s'appuient sur des procédés d'intelligence artificielle pour analyser un nombre important de données en fonction de critères prédéfinis, les connexions inquiétantes pouvant ensuite donner lieu à des vérifications ciblées au moyen de l'identification de la personne en cause et du recueil des données de connexion afférentes.

19. Voir l'article L. 851-3 du code de la sécurité intérieure.

20. Voir les articles 15 et 18 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

21. Voir point 1.2.1 du rapport d'activité.

1.1.2. Le développement de l'usage des SIA en matière de renseignement apparaît inéluctable : la quête de l'efficience

Le développement du recours aux SIA dans le processus de renseignement apparait indispensable pour en assurer l'efficience à l'avenir face à trois contraintes incontournables.

Il relève tout d'abord d'une nécessité technique face à la « révolution de la donnée ». L'essor de l'IA intervient en effet dans un contexte marqué par une « mise en données » (ou « *datafication* »[22]) touchant l'ensemble des activités humaines et conduisant à une croissance exponentielle de la production de données de sorte qu'avec les ressources humaines disponibles, il n'est possible de traiter qu'une petite - voire bientôt infime - partie des données disponibles. L'IA constitue donc un levier essentiel de maîtrise du monde numérique de demain[23].

Dans le domaine du renseignement, le recours aux SIA s'impose ainsi pour permettre aux agents des services d'appréhender la masse de données, de naviguer au sein de celle-ci et de mieux l'exploiter afin d'être en mesure de se concentrer sur l'analyse utile des éléments à disposition et de garantir l'efficacité de leur intervention. La Commission nationale de l'informatique et des libertés (CNIL) résume ainsi les liens consubstantiels entretenus par la donnée et les SIA d'apprentissage automatique par la formule « *L'algorithme sans données est aveugle. Les données sans algorithmes sont muettes* »[24].

22. Terme introduit en 2013 par Kenneth Cukier et Victor Mayer-Schöenberger dans leur essai, *The rise of big data.* « Datafier » un phénomène vise à le transformer en données quantifiées, tabulées et analysables.

23. Comme le conclut la mission menée par Cédric Villani sur l'intelligence artificielle, les technologies d'IA « *déterminent notre capacité à organiser les connaissances, à leur donner un sens, à augmenter nos facultés de prise de décision et de contrôle des systèmes* ». Voir le rapport *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, publié le 28 mars 2018.

24. CNIL, synthèse du débat public, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle,* 15 décembre 2017

Le développement de l'usage des SIA n'est pas seulement une réponse technique à la révolution numérique. Il résulte aussi d'une adaptation nécessaire de l'action des services de renseignement à de nouvelles formes de menaces.

Depuis le début du siècle, les menaces se sont en effet fortement diversifiées et ne résultent plus seulement d'adversaires étatiques combattant au moyen de forces armées traditionnelles.

Une mouvance terroriste aux ramifications mondiales s'est ainsi développée, engendrant une menace disséminée et protéiforme, appelant à une automatisation et une généralisation poussée des procédés de surveillance.

De même, les possibilités offertes par l'essor d'Internet et les nouveaux outils numériques de communication, permettent à nos ennemis de mettre en réseau leurs actions, de mieux les dissimuler et de contourner les surveillances. Les « écoutes téléphoniques » qui constituaient par le passé la technique de surveillance de référence sont ainsi devenues bien moins productives du fait du recours massif aux messageries et applications chiffrées. D'autres techniques, bien que plus récentes, se heurtent aussi aux évolutions technologiques qui questionnent leur efficacité. L'usage des SIA apparait dans ce cadre comme un outil nécessaire pour accroitre, ou du moins préserver, l'efficacité des techniques légales de renseignement.

Par ailleurs, les pouvoirs publics sont aujourd'hui confrontés à de nouvelles formes de criminalités et à des formes inédites de conflits qui se développent dans l'espace cyber. La « petite » délinquance comme la criminalité organisée y ont trouvé aussi bien des moyens de faciliter leur action que de nouvelles opportunités délictuelles et criminelles (escroqueries en ligne, cyberattaques, notamment). Les puissances étatiques ou organisations liées y ont, elles aussi, trouvé un nouveau terrain de combat, permettant d'engager des luttes informationnelles ou des tentatives de déstabilisation.

La capacité à disposer de SIA concurrentiels apparaît donc déterminante pour maintenir les capacités d'information, d'intervention et d'analyse des services de renseignement face à la diversification des risques et des menaces, y compris technologiques, et écarter toute asymétrie entre leurs moyens et ceux des adversaires. L'essor de l'usage de l'IA en matière de renseignement est ainsi essentiel pour préserver les capacités tant défensives (détection des attaques, menaces, crimes ou délits) qu'offensives (ripostes) de l'État. Dans un contexte de compétition internationale marquée pour le développement et la maitrise des procédés d'IA, un décrochage des services nationaux en la matière ferait finalement peser le risque d'une perte de souveraineté.

1.2. Le déploiement des SIA s'opère dans un cadre juridique incomplet

Alors même que l'emploi des SIA est appelé à s'étendre, la réglementation de l'IA demeure aujourd'hui balbutiante sur la scène internationale comme au niveau national.

1.2.1. Le foisonnement des réflexions et règles de droit souple face aux risques inhérents au développement des SIA...

Entre enthousiasme face aux prouesses récentes et aux bénéfices attendus de nouveaux outils numériques « intelligents » au plan économique et sociétal et crainte d'un asservissement de l'humain par la machine ou d'une surveillance généralisée, l'essor de l'IA questionne certains des grands principes et équilibres qui fondent la vie démocratique.

Ces interrogations et inquiétudes se sont traduites durant la dernière décennie par un foisonnement de réflexions sur les risques inhérents à son développement. En réponse, les initiatives, publiques ou privées,

visant à définir un référentiel éthique de l'intelligence artificielle ou poser des principes directeurs applicables en ce domaine se sont multipliées.

Les propositions de charte, guide, ou autres recommandations, émanant d'acteurs étatiques, d'organisations internationales, d'institutions académiques et de recherche mais aussi d'entreprises[25] ou de personnalités[26], mettant en avant les enjeux inhérents au développement de l'IA et exposant de grands principes éthiques, sont ainsi trop nombreuses pour être inventoriées. Tout au plus peut-on souligner un **mouvement tendant à poser les jalons d'une gouvernance internationale de l'intelligence artificielle, au moyen de l'adoption d'une « éthique » spécifique**.

Au niveau international, ce mouvement s'est traduit en particulier, par l'adoption de plusieurs propositions de recommandation ou chartes, sans portée juridique contraignante, formalisant l'accord de divers États sur les usages recommandés, ou inversement à proscrire, de l'IA.

Point d'orgue de ce mouvement, le Secrétaire général des Nations Unies a annoncé en novembre 2023 la création d'un nouvel organisme consultatif sur l'IA pour soutenir les efforts de la communauté internationale visant à gouverner cette nouvelle technologie, soulignant la nécessité d'organiser « *une conversation mondiale, multidisciplinaire et multipartite sur les risques et les défis, les opportunités et la gouvernance de l'IA* » et l'impératif d'une régulation mondiale des technologies émergentes d'IA basée sur les principes fondamentaux de la Charte des Nations Unies et le plein respect des droits humains.

25. Voir en particulier le « Partenariat pour l'intelligence artificielle au bénéfice des citoyens et de la société » conclu en septembre 2016 entre Google, Facebook, IBM, Microsoft et Amazon pour définir les bonnes pratiques, notamment en termes d'éthique, dans le domaine de l'IA, ou encore la Charte éthique de l'IA adoptée et publiée par Google en 2018.

26. Du monde scientifique en particulier. À titre d'exemple, plus de deux milles personnalités, dont Stephen Hawking et Elon Musk ont adopté à l'issue d'une conférence organisée à en janvier 2017, à Asilomar (Californie), un « *Guide de référence pour un développement éthique de l'intelligence artificielle* », édictant 23 principes fondamentaux ayant vocation à encadrer ce développement.

LES PRINCIPAUX TEXTES NON CONTRAIGNANTS ADOPTÉS AU NIVEAU INTERNATIONAL

La Déclaration de Bletchley[27] pour une IA responsable : signée le 1er novembre 2023 au Royaume-Uni par 28 États (dont les États-Unis, les membres de l'Union européenne et la Chine), cette déclaration officialise l'accord des pays participants pour travailler ensemble à l'établissement d'un cadre garantissant que les technologies d'IA soient développées et utilisées de manière responsable et sûre, « centrée sur l'humain », et que les risques potentiellement « catastrophiques » issus des progrès en la matière soient contenus. Ce texte est l'initiative la plus récente de coopération internationale appelant à encadrer les défis et opportunités que présente l'IA.

Les principes directeurs et le code de bonne conduite volontaire des pays du G7 : ce texte, adopté le 30 octobre 2023 par les dirigeants des pays du G7, fixe des principes généraux et énumère 11 recommandations non contraignantes applicables aux organisations qui développent des systèmes d'IA avancés, visant au développement d'une IA « sûre, sécurisée et digne de confiance ».

La Recommandation de l'UNESCO sur l'éthique de l'IA : adoptée le 23 novembre 2021 par les 193 États membres de l'UNESCO réunis en Conférence générale, cette recommandation rappelle l'impératif de protection des droits de l'homme et de la dignité de la personne humaine, invite au respect dans le déploiement de l'IA de principes fondamentaux tels que la transparence et l'équité, et consacre l'importance de la responsabilité humaine dans le contrôle des systèmes d'intelligence artificielle. Elle invite les États membres à prendre les mesures appropriées, notamment législatives, permettant de garantir le respect des principes et normes qu'elle énonce.

27. Bletchley Park est une ancienne base du bureau anglais responsable de l'interception et du déchiffrage des communications étrangères d'espionnage (*Government Code and Cypher School*) où officièrent notamment Alan Turing et les décrypteurs ayant maîtrisé la machine Enigma.

La recommandation de l'OCDE sur l'intelligence artificielle : cette recommandation, adoptée par le Conseil de l'OCDE le 22 mai 2019 et amendée le 8 novembre 2023, reconnait que « *l'IA promet d'améliorer la prospérité et le bien-être des individus, de contribuer à une activité économique mondiale dynamique et durable, de stimuler l'innovation et la productivité, et d'aider à affronter les grands défis planétaires* **», tout en admettant que son développement met à l'épreuve «** *la démocratie et les droits de l'homme, la protection de la vie privée et la confidentialité des données, et la sécurité numérique* **». Elle fixe les principes d'une approche responsable en appui d'une IA digne de confiance, précisant que les acteurs de l'IA devraient notamment «** ***respecter l'État de droit, les droits de l'homme et les valeurs démocratiques tout au long du cycle de vie des systèmes d'IA*** **»** et s'engager à assurer la transparence et le caractère explicable de leur SIA.

Aux niveaux européen et français, les réflexions éthiques et juridiques comme les propositions d'encadrement sont tout aussi abondantes depuis plusieurs années.

Le Conseil de l'Europe s'est ainsi doté en juin 2019 d'un Comité sur l'intelligence artificielle[28], chargé par le Comité des ministres d'élaborer une convention-cadre sur le développement, la conception et l'application de l'intelligence artificielle, fondée sur les normes du Conseil de l'Europe en matière de droits de l'homme, de démocratie et d'État de droit. Les premières réflexions de ce groupe sur les principes d'un cadre juridique pour l'intelligence artificielle ont été publiées en décembre 2021[29].

L'Union Européenne a quant à elle débuté ses réflexions sur l'intelligence artificielle avec l'adoption dès le mois d'avril 2018 de sa communication sur « *L'intelligence artificielle pour l'Europe* », annonçant un plan coordonné dans le domaine de l'IA, suivie, dans la foulée, de la mise en place en juin 2018 d'un comité consultatif de 52 experts indépendants,

28. Comité *ad hoc* sur l'intelligence artificielle (CAHAI), remplacé en 2021 par le Comité sur l'intelligence artificielle (CAI).

29. Rapport sur les « *Éléments potentiels d'un cadre juridique sur l'intelligence artificielle, fondés sur les normes du Conseil de l'Europe en matière de droits de l'homme, de démocratie et d'État de droit* ».

le Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle[30], ayant pour mission de fournir des expertises, des conseils stratégiques et des propositions pour développer « *une intelligence artificielle digne de confiance* ». Les travaux de ce groupe[31], dont le mandat s'est achevé en juillet 2020, ont notamment servi de ressources aux initiatives d'élaboration de la politique numérique de l'Union Européenne, ainsi qu'à l'élaboration d'une législation en matière d'IA, adoptée le 21 mai 2024 (voir point 1.2.2 ci-dessous).

S'agissant plus spécifiquement de l'étude des incidences de l'IA sur la garantie des droits, l'Agence des droits fondamentaux, chargée de fournir une assistance en ce domaine aux institutions et autorités de l'Union, a publié plusieurs études analysant son impact sur les droits et libertés, notamment les risques de la reconnaissance faciale et les biais et discriminations générés par les algorithmes[32] et proposant des lignes directrices à retenir.

En France, les réflexions publiques sont aussi très abondantes. De nombreux rapports et études examinant les enjeux entourant l'essor de l'IA se sont ainsi succédés au cours de la dernière décennie, les réflexions étant surtout axées sur les enjeux éthiques et, dans une moindre mesure, juridiques. Témoignent notamment de cette priorité donnée aux considérations éthiques les propositions de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur l'IA déposées en mars 2017[33], l'étude de la CNIL sur les enjeux éthiques des algorithmes et de l'intelligence artificielle de décembre 2017[34] et le rapport de Cédric Villani de mars 2018[35], qui a ouvert la voie au lancement de la *stratégie nationale pour l'intelligence artificielle* fin 2018.

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

31. Voir notamment le rapport *Lignes directrices en matière d'éthique pour une IA digne de confiance*, publié le 8 avril 2019.

32. Rapports intitulés *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019 et *Bias in algorithms - Artificial intelligence and discrimination*, 8 décembre 2022.

33. Rapport n° 464, *Pour une intelligence artificielle maîtrisée, utile et démystifiée*, tome I, déposé le 15 mars 2017.

34. Précité, note 24.

35. Précité, note 23.

1.2.2. | ... contraste avec l'absence de réglementation générale des techniques d'IA en droit positif

Si ces dernières années ont vu se multiplier les instruments de droit souple, répondant le plus souvent à la préoccupation d'une utilisation « **éthique** » de l'IA, cette technologie s'est développée jusqu'à présent hors de tout cadre juridique spécifique.

Certes, **les instruments généraux, internationaux, européens ou nationaux, de protection des droits fondamentaux ont vocation à s'appliquer à tous les domaines de la vie, quelle que soit la technologie utilisée et donc également aux SIA**.

Pour ce qui est de la France, les grands principes, droits et libertés consacrés par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, la Charte des droits fondamentaux de l'Union Européenne et le bloc de constitutionnalité, notamment le droit au respect de la vie privée, la liberté d'expression et de réunion, ou encore les principes d'égalité et de non-discrimination, peuvent venir encadrer le recours à des technique utilisant l'IA, en particulier dans leur usage par les autorités publiques dans le champ de la sécurité. Quelques règles spécifiquement applicables aux SIA ont ainsi pu être dégagées sur le fondement de ces principes, notamment en matière de surveillance.

QUELQUES EXEMPLES D'APPLICATION DES DROITS FONDAMENTAUX AUX TECHNIQUES DE SURVEILLANCE ET RENSEIGNEMENT UTILISANT DES SIA DANS LA JURISPRUDENCE EUROPÉENNE

Conséquences des évolutions technologiques :

Dès 2008, la Cour européenne des droits de l'Homme (CEDH) a précisé, dans une affaire mettant en jeu le prélèvement et la conservation de données biologiques par des autorités publiques à des fins de prévention de la criminalité, que l'usage des techniques scientifiques modernes devait nécessairement être apprécié au regard d'une mise en balance des avantages pouvant résulter du recours à ces techniques et du respect des droits fondamentaux des individus, en l'espèce les intérêts essentiels s'attachant à la protection de la vie privée. Dès lors, l'État revendiquant l'utilisation de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière. Dans cette affaire, la Cour souligne que le rythme élevé auquel se succèdent les innovations dans le domaine de la génétique et des technologies de l'information fait naitre des risques d'atteinte à la vie privée par des voies nouvelles, que l'on ne peut prévoir aujourd'hui avec précision (CEDH, *S. et Marperc.Royaume-Uni*, n° 30562/04 et 30566/04, 4 décembre 2008).

Surveillance de masse :

Dans une affaire relative à la surveillance de masse des communications, la CEDH a examiné le recours par les gouvernements à des technologies de pointe leur permettant d'intercepter un très grand nombre de données, afin de lutter contre les formes nouvelles prises par le terrorisme. Elle a censuré en l'espèce la réglementation hongroise en raison de l'atteinte disproportionnée au droit au respect de la vie privée qu'elle permettait et de l'absence de recours effectif (CEDH, 12 janvier 2016, *Szabó et Vissy c.Hongrie*, **n° 37138/14,).**

Par la suite, dans deux arrêts du 25 mai 2021, la grande chambre de la CEDH s'est penchée sur les conditions dans lesquelles un régime de surveillance de masse des communications électroniques, qui peut inclure des outils d'IA,

est compatible avec les articles 8 (droit au respect des correspondances et de la vie privée) et 10 (liberté d'expression) de la Convention (CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n^{os} 58170/13, 62322/14 et 24960/15, et 25 mai 2021, *Centrum för Rättvisa c. Suède*, n° 35252/08).

Reconnaissance faciale :

Dans une affaire portant sur la conservation sans durée des données personnelles (profil ADN, empreintes digitales et photographie), la CEDH relève que le développement rapide de techniques de plus en plus sophistiquées permettant, entre autres, la reconnaissance ou la cartographie faciale à partir de photographies d'individus, rend la captation de leur image et la conservation des données recueillies problématiques. Elle souligne que le caractère complexe des technologies utilisées doit être pris en compte dans l'examen de la nécessité de l'ingérence dans le droit au respect de la vie privée de l'individu dont l'image a été captée (CEDH, 13 février 2020, *Gaughran c. Royaume-Uni*, n° 45245/15).

En dehors de l'application de ces instruments généraux protégeant les droits et libertés fondamentaux, le recours aux SIA n'est pour l'heure encadré par aucune réglementation générale spécifique. Le développement de ces derniers n'est ainsi régi, en droit européen comme en droit national, que par des dispositions dispersées édictées dans d'autres matières.

S'agissant de l'Union européenne, il y a toutefois lieu de relever l'adoption récente d'une législation visant à encadrer spécifiquement l'intelligence artificielle, le projet d'*AI Act*. Sur la base d'une proposition législative présentée par la Commission européenne le 21 avril 2021, un accord provisoire entre le Conseil et le Parlement européen a été trouvé le 9 décembre 2023 sur un projet de règlement fixant des règles harmonisées concernant l'intelligence artificielle et visant, tout à la fois, à stimuler l'investissement et l'innovation en ce domaine et à encadrer les systèmes d'IA pour assurer le bon fonctionnement du marché intérieur et garantir des standards élevés en matière d'éthique et de respect des droits fondamentaux.

Le projet d'AI ACT a été adopté par le Parlement européen le 13 mars 2024 et par le Conseil européen le 21 mai suivant.

Ce projet, dont le champ d'application est très large du fait d'une définition englobante des systèmes d'intelligence artificielle et de l'étroitesse des domaines d'exclusion, retient une approche par les risques conduisant à proscrire les SIA présentant un risque inacceptable, à imposer des contraintes fortes sur les SIA à haut risque et à ne soumettre les autres systèmes qu'à des obligations légères. Les règles retenues pour les différents SIA s'accompagnent de la mise en place d'un système révisé de gouvernance et de mécanismes spécifique de sanctions en cas de violation de la législation.

Le règlement **établissant des règles harmonisées concernant l'intelligence artificielle** (*AI Act*), dont l'entrée en vigueur est prévue pour 2026, sera l'une des toutes premières législations générales applicables sur l'IA au monde avec celle récemment mise en œuvre aux États-Unis[36].

36. Avec l'adoption du *National Artificial Intelligence Initiative Act* (NAIIA) en 2020 et du décret présidentiel *Safe, Secure, and Trustworthy Artificial Intelligence* en octobre 2023.

LES GRANDES LIGNES DU RÈGLEMENT ÉTABLISSANT DES RÈGLES HARMONISÉES CONCERNANT L'INTELLIGENCE ARTIFICIELLE (*AI ACT*) ADOPTÉ PAR LE PARLEMENT EUROPÉEN ET LE CONSEIL

Champ d'application :

Le règlement, qui sera pleinement applicable en 2026 retient une définition assez large des techniques qu'il a vocation à encadrer. Il définit le système d'intelligence artificielle comme « *un système automatisé conçu pour fonctionner à différents niveaux d'autonomie, qui peut faire preuve d'une capacité d'adaptation après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, la manière de générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels* » (art. 3 (1) du chapitre I[37]).

Le règlement a vocation à s'appliquer à tous les SIA mis sur le marché ou en service dans l'Union, ou utilisés par un utilisateur présent ou établi dans l'Union, et édicte des obligations particulières pour les fournisseurs (développeurs) ou utilisateurs (« déployeurs ») de systèmes d'IA. Toutefois, il ne s'appliquera pas aux systèmes d'IA utilisés à des fins militaires, de défense ou de sécurité nationale, ces domaines ne relevant pas du champ d'application du droit de l'UE. Il n'affectera pas les compétences des États membres en matière de sécurité nationale, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches liées à ces compétence (art. 2.3 du chapitre I[38]). Il n'aura pas non plus vocation à régir les systèmes utilisés aux seules fins de recherche et d'innovation (art. 2.6 du chapitre I)

37. Suivant la numérotation provisoire disponible au moment de l'impression du présent rapport.
38. Suivant la numérotation provisoire disponible au moment de l'impression du présent rapport.

Classification des systèmes d'IA :

Le règlement classe les SIA en fonction des risques qu'ils présentent :

Les SIA interdits (art. 5 du chapitre II[39]) :

Le texte prévoit d'interdire les SIA présentant un risque inacceptable. Considérées comme une menace claire pour les droits fondamentaux des personnes, les pratiques suivantes, qu'elles soient ou non intentionnelles, sont interdites : les techniques relevant de la manipulation comportementale cognitive ; les méthodes exploitant les vulnérabilités liées à l'âge, au handicap, ou à la situation économique ou sociale ; les méthodes de notation sociale portant évaluation ou classification d'individus ou de groupes sur la base de leur comportement social ou de leurs traits personnels ; l'évaluation du risque qu'une personne commette des infractions pénales sur la seule base d'un profilage ou de traits de personnalité, sauf exception encadrée ; la constitution de bases de données de reconnaissance faciale par extraction non ciblée d'images faciales sur internet ou d'images de vidéosurveillance et l'identification biométrique à distance en temps réel dans des lieux publics, sous réserve des exceptions déterminées par le règlement pour leur usage par les forces de l'ordre.

Les SIA à haut risque (chapitre III[40]) :

Cette catégorie regroupe des systèmes utilisés dans des secteurs industriels énumérés (notamment aviation civile, transports…) ou identifiés comme étant par nature à haut risque et listés en annexe (notamment les systèmes biométriques et les systèmes d'aide aux autorités répressives). Sont également classés comme présentant un risque élevé les SIA qui établissent des profils de personnes (traitements automatisés de données personnelles utilisés pour évaluer divers aspects de la vie d'une personne, tels que ses performances professionnelles, sa situation économique ou, sa santé, notamment).

39. Suivant la numérotation provisoire disponible au moment de l'impression du présent rapport.

40. Suivant la numérotation provisoire disponible au moment de l'impression du présent rapport.

La mise sur le marché ou en service et l'utilisation de ces SIA à haut risque est encadrée par des obligations spécifiques destinées à garantir leur fiabilité et leur innocuité, notamment en termes de contrôle humain sur la machine, d'établissement d'une documentation technique, de mise en place d'un système de gestion du risque. De plus, une analyse d'impact sur les droits fondamentaux doit être effectuée avant qu'un système d'IA à haut risque ne soit mis sur le marché.

Les modèles d'IA à usage général (GPAI) :

Le règlement prévoit un régime particulier pour les GPAI, qui se caractérisent par leur grande généralité et leur capacité à exécuter avec compétence un large éventail de tâches distinctes, quelle que soit la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval. Ces modèles doivent respecter des obligations de transparence spécifiques avant leur mise sur le marché, des règles plus strictes étant prévues pour ceux de ces modèles qui sont considérés comme systémiques, incluant une évaluation des risques systémiques et une obligation de protection de la cyber sécurité.

Les autres SIA :

Les systèmes d'IA qui présentent un risque minimal ne sont soumis à aucune obligation spécifique au titre du règlement, en dehors d'une obligation de transparence peu contraignante.

Gouvernance :

Le texte prévoit notamment la création d'un Bureau de l'IA (ou *Office AI*) au sein de la Commission européenne et d'un Comité européen de l'intelligence artificielle réunissant les représentants des État et le Contrôleur européen de la protection des données en qualité d'observateur. Il comporte en outre des règles concernant la désignation des autorités nationales compétentes, notamment une autorité « notifiante » et les autorités de surveillance du marché, pour assurer la mise en œuvre du règlement. Ces autorités auront en particulier pour mission de représenter l'État-membre au sein du comité européen de l'IA, d'accréditer et évaluer les organismes de conformité et de veiller au bon fonctionnement du marché des SIA.

Toutefois, outre que l'*AI Act* ne s'appliquera pas dans son intégralité avant 2026, cette nouvelle réglementation ne couvrira pas l'ensemble des sujets soulevés par le recours accru aux SIA dans le champ de l'action publique. En particulier, elle ne s'appliquera pas en matière de renseignement en raison de l'exclusion de son champ d'application des domaines de la défense et de la sécurité nationale.

De fait, l'encadrement actuellement applicable aux SIA résulte de la juxtaposition de diverses règles, dont la cohérence d'ensemble reste à bâtir.

En dehors des normes supérieures, constitutionnelles ou conventionnelles, imposant le respect des droits et liberté fondamentaux, les dispositions applicables aux SIA relèvent des législations sectorielles qui concernent ses composants matériels (logiciels, équipements, etc.) ou certains des procédés utilisés (traitements de données, algorithme, etc.).

Sur ce second volet, le plus sensible, les SIA sont essentiellement concernés par la réglementation relative au **traitement des données à caractère personnel**[41].

Tout SIA utilisant des données à caractère personnel constitue ainsi un **traitement de données à caractère personnel** au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui précise dans son premier article que : « *L'informatique doit être au service de chaque citoyen. […]. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* ». Les SIA doivent respecter les droits accordés aux individus d'accéder aux données à caractère personnels les concernant, de les faire rectifier et de faire une démarche d'opposition fixés, selon le cas, par le règlement général sur la protection des données personnelles (RGPD)[42], par le titre III de la loi du 6 janvier 1978 pour les traitements relevant de la directive dite police-justice[43], et du titre IV de cette même loi pour les traitements ne relevant pas du champ du droit de l'Union, notamment ceux qui

41. Pour un exposé exhaustif, voir annexe 10 de l'étude précitée du Conseil d'État, note 9.

42. 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

43. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

intéressent la défense et la sûreté de l'État à l'instar des traitements utilisés par les services de renseignement.

Par ailleurs, lorsque sont en cause des systèmes publics, s'applique également un corpus de règles visant à assurer la **transparence de l'action publique**. Deux dispositifs sont principalement concernés.

Tout d'abord, en application du code des relations entre le public et l'administration, les usagers bénéficient d'un droit d'accès général aux documents administratifs, qui leur permet de demander communication des éléments structurants des SIA tels que les fichiers, codes-sources, ou la documentation technique achevée relative à un SIA utilisé dans le cadre d'une mission de service public.

Ensuite, le RGPD, la loi du 6 janvier 1978 et le code des relations entre le public et l'administration ont prévu un encadrement particulier des décisions administratives fondées sur un traitement algorithmique - qualifiées de « décisions automatisées » - lorsqu'elles sont édictées sur le seul fondement d'un tel traitement. À cet égard, l'article 47 de la loi interdit par principe qu'une décision qui produit des effets juridiques à l'égard d'une personne ou l'affecte de manière significative soit prise sur le seul fondement d'un traitement automatisé, sauf, notamment, s'il s'agit d'une décision administrative individuelle, ladite décision devant lors obligatoirement mentionner qu'elle été fondée sur un traitement algorithmique. Une telle possibilité est exclue pour les décisions entrant dans le champ de la directive police-justice si elle n'est pas entourée de garanties appropriées, et au minimum du droit d'obtenir une intervention humaine. Le code des relations entre le public et l'administration prévoit pour sa part une information renforcée des usagers lorsqu'est en cause une décision fondée sur un traitement algorithmique, que l'on soit en présence d'une « décision automatisée » ou simplement d'une décision assistée par un traitement[44].

Enfin, le code des relations entre le public et l'administration fait obligation aux administrations de plus de 50 agents de publier en ligne, de manière spontanée, les règles définissant les principaux traitements

44. Une telle décision doit comporter mention du fait qu'elle a été prise sur la base d'un traitement algorithmique et l'administration est tenue, en cas de demande de l'intéressé de lui communiquer, sous une forme intelligible, les règles définissant ce traitement et les principales caractéristiques de sa mise en œuvre

algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles[45].

S'agissant plus spécifiquement du renseignement, l'encadrement juridique des SIA employés apparaît là aussi limité.

D'une part, en ce qui concerne les traitements des données à caractère personnel, les techniques utilisées en matière de renseignement relèvent en effet d'un régime dérogatoire ne prévoyant, au mieux, qu'un accès indirect aux données à caractère personnel contenues dans les fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique[46] étant précisé qu'elles sont également hors du champ d'application du RGPD et de la directive police-justice. En ce qui concerne les obligations de transparence de l'action publique, elles sont d'évidence écartées pour les surveillances secrètes, eu égard à leur objet même.

D'autre part, l'utilisation de l'intelligence artificielle n'est pas spécifiquement réglementée par le livre VIII du code de la sécurité intérieure, qui, en dehors de la consécration d'une utilisation particulière de l'algorithme à son article L. 851-3 (voir point 1.1 ci-dessus), n'évoque que de manière incidente les techniques d'intelligence artificielle.

Seul l'article L. 854-2 fait ainsi mention expresse de la possibilité pour les services de renseignement de mettre en œuvre un traitement automatisé, pour l'exploitation des données de connexion interceptées dans le cadre de la surveillance internationale. Il y a néanmoins lieu de considérer que le III de l'article L. 822-2 du code de la sécurité intérieure, en autorisant des « programmes de recherche », vise à permettre l'utilisation d'outils de l'IA pour les besoins de la recherche-développement en matière de techniques de recueil et d'exploitation des renseignements[47].

Faute d'encadrement juridique précis, l'emploi de l'IA en matière de renseignement impose de fait un travail délicat d'interprétation des principes et règles juridiques existants, édictés sans prise en compte des problématiques spécifiques soulevées par les évolutions technologiques.

45. Voir l'article L. 312-1-3 du CRPA.

46. Les garanties prévues par le régime général du droit d'accès et de rectification sont en effet incompatibles avec les traitements dits de « souveraineté ».

47. Il ressort en effet des débats parlementaires que l'introduction, par l'article 10 de la loi n° 2021-998 du 30 juillet 2021 de ces dispositions dérogeant aux règle générales de conservation des données résultait de la prise en compte des besoins des outils d'intelligence artificielle, notamment des algorithmes (voir notamment sur ce point le rapport des sénateurs M. Marc-Philippe Daubresse et de Agnès Canayer, n° 694 du 16 juin 2021).

2. Les défis soulevés par l'accélération de l'emploi des SIA dans le domaine du renseignement appellent une vigilance particulière et un contrôle renforcé

2.1. Des risques et des enjeux spécifiques en matière de renseignement

L'emploi des SIA en matière de sécurité nationale, et singulièrement dans le domaine du renseignement, soulève des questionnements éthiques majeurs et des enjeux particuliers qu'il convient de circonscrire.

2.1.1. | Les risques de l'automatisation

L'essor de l'usage de l'IA dans le domaine de la sécurité et de l'ordre public fait régulièrement ressurgir la crainte d'une surveillance de masse de la population par les autorités publiques.

L'IA repose fondamentalement sur l'automatisation, qui a pour fonction d'optimiser et d'accélérer un processus en remplaçant l'homme. Aujourd'hui, les technologies d'automatisation permettent la captation et l'exploitation massive et rapide de données. Si l'on y ajoute le fait que les outils d'IA les plus récents peuvent être utilisés en mobilité et interconnectés, une surveillance généralisée des populations parait à portée de main.

Dès lors, l'emploi des nouvelles technologies en matière sécuritaire peut être perçu, non comme un facteur de promotion de la sécurité collective, mais comme un instrument de la surveillance de masse, sentiment nourri par la méfiance que ressent une partie de la population vis-à-vis de l'État et de ses fonctions régaliennes.

Les pratiques de certains gouvernements ont, il est vrai, montré les capacités des nouvelles technologies de surveillance. Emblématique en la matière, le régime communiste chinois a développé un projet inédit de surveillance de ses citoyens, s'appuyant en particulier sur le déploiement d'un système de crédit social, dispositif de contrôle permanent des individus se basant sur l'intelligence artificielle et le « *Big Data* ».

Sans verser dans la crainte de la reproduction généralisée d'un tel modèle, la démultiplication de la surveillance que permet l'automatisation comporte toutefois intrinsèquement un risque majeur d'atteinte au droit au respect de la vie privée, notamment de protection des données personnelles, et menace par ricochet la liberté d'expression par le phénomène d'autocensure que le déploiement de dispositifs de surveillance peut engendrer, influant ainsi sur les comportements et l'équilibre psychologique des individus (« *chilling effect* »). Si la plupart des SIA développés n'ont ni pour objet ni pour effet de modifier les conditions dans lesquelles les données sont recueillies, ils permettent en effet une analyse systématique et automatisée de ces dernières de nature à accroître considérablement le nombre et la précision des informations qui peuvent en être extraites.

Autre conséquence de l'automatisation, à côté de la démultiplication des possibilités de surveillance, la perte du contrôle humain est souvent mise en exergue pour pointer les dangers des SIA.

L'un des questionnements les plus essentiels que soulève l'utilisation des outils d'IA tient aux conséquences de la délégation à une « machine » de la prise de décisions critiques ou encore à la délégation massive de décisions non critiques.

À cet égard, l'accent est d'abord mis sur le risque de déresponsabilisation de l'agent « décideur », ainsi que sur les biais introduits dans sa décision, les SIA n'étant jamais neutres puisqu'ils sont paramétrés par l'homme en incorporant inévitablement des partis pris.

Une telle difficulté se pose dans le domaine du renseignement comme dans le reste du champ de l'action publique, avec toutefois une acuité particulière du fait de la sensibilité de la matière. En dehors du cas particulier de la technique de l'algorithme, l'encadrement juridique de la mise en œuvre des techniques de renseignement est en effet centré sur l'exploitation humaine des données recueillies et fait ainsi reposer sur une personne la responsabilité de vérifier la finalité d'intérêt public poursuivie, le caractère fondé d'une surveillance et la proportionnalité de l'ingérence dans les droits et libertés fondamentaux à la menace ou aux enjeux en cause.

L'usage d'outils de SIA, rapides et puissants, peut laisser craindre que les technologies ne soient pas qu'une simple aide à la prise de décision mais se substituent à l'agent dans sa tâche, celui-ci se bornant à entériner les résultats proposés par la machine. Un hiatus pourrait de ce fait voir le jour entre une responsabilité ressentie de l'agent et sa responsabilité juridique, notamment pénale, telle qu'elle est fixée par l'article L. 862-2 du code de la sécurité intérieure.

En outre, la perte de contrôle humain prend une dimension particulière avec les développements de l'IA générative. En effet, les SIA basés sur des procédés d'apprentissage profond ou même seulement sur des algorithmes particulièrement complexes se caractérisent par leur opacité.

Ces SIA peuvent vite s'avérer trop compliqués pour pouvoir être présentés et compris par les agents chargés de les utiliser. Au-delà de ces agents, l'opacité des SIA représente un défi particulier pour les personnes et autorités chargées de les contrôler. Elle pourrait même questionner le droit à un recours juridictionnel effectif, qui nécessite une compréhension

suffisante des technologies par l'autorité juridictionnelle pour permettre le rendu d'une décision juste.

La capacité à expliquer[48] le fonctionnement des systèmes constitue aujourd'hui l'un des grands enjeux associés à l'essor de l'IA et soulève la question de la maîtrise et de la possibilité d'auditer les procédés de surveillance mis en œuvre.

2.1.2. Des enjeux spécifiques de gestion de la donnée et de cohérence du cadre juridique

Le développement de l'usage des SIA par les services de renseignement soulève deux enjeux spécifiques qui tiennent à la gestion de la donnée et à la cohérence du cadre juridique en vigueur.

L'introduction des SIA interroge les principes de gestion des données posés par le législateur afin de préserver l'équilibre entre les nécessités d'intérêt public auxquelles répond la politique publique du renseignement et la préservation des droits et libertés fondamentaux, en particulier le respect de la vie privée.

Pour assurer cet équilibre, les dispositions en vigueur du code de la sécurité intérieure déterminent strictement les modalités d'utilisation des données recueillies par les services de renseignement, y compris dans le cadre de la recherche-développement, fixent les durées de conservation de chaque type de données, encadrent leur possibilité de partage, au sein et en dehors de la communauté du renseignement, et limitent les possibilités de croisement des différents fichiers de police administrative.

Or, l'utilisation massive, partagée et croisée des données est consubstantielle au développement de l'IA d'apprentissage automatique. Les SIA sont en effet d'autant plus performants qu'ils sont nourris

48. Voir notamment l'analyse concernant l'IA d'apprentissage dans le rapport Villani précité, voir note 23.

par un important jeu de données, de nature variée, et qu'ils peuvent les traiter sans condition particulière ni limitation de durée. La mise à disposition des acteurs du numérique de gisements de données de masse est d'ailleurs l'une des considérations qui a poussé à l'adoption, au niveau européen, d'un paquet législatif relatif à la gouvernance des données, composé d'un règlement sur la gouvernance des données (*Data Governance Act*) et d'un règlement sur la donnée (*Data Act*)[49]. Destinée à promouvoir l'accès, le partage et la réutilisation responsables, dans le respect des valeurs de l'Union européenne, des données (données ouvertes, informations du secteur public, ou données personnelles), cette législation met en place un environnement présenté comme nécessaire à la réussite de la stratégie européenne en matière d'intelligence artificielle.

LES GRANDS PRINCIPES DES RÈGLEMENTS SUR LES DONNÉES

Le règlement sur la gouvernance des données, applicable depuis le 24 septembre 2023, et le règlement sur les règles harmonisées en matière d'accès et d'utilisation équitables des données, qui sera lui applicable à compter du 12 septembre 2025, fixent la stratégie européenne sur les données. Ils visent à renforcer la compétitivité et la souveraineté de l'UE dans ce domaine 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 RGDP.

49. Voir le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 [*règlement sur la gouvernance des données*] et le 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 et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 [règlement sur les données].

Ils posent en particulier les principes :
- d'une équité entre les acteurs économiques dans l'utilisation des données générées par les objets connectés ;
- de la possibilité pour les entreprises de réutiliser les données détenues par les organismes du secteur public, y compris les données dites « à caractère protégé » après anonymisation ;
- de l'accès des organismes du secteur public aux données privées, en cas de besoins exceptionnels ;
- de la fixation de règles pour faciliter le passage des données entre les fournisseurs de services et les entreprises de traitement de données.

Les règles posées par le code de la sécurité intérieure, qui tendent à minimiser tant la collecte des données que leurs possibilités de conservation et de partage, peuvent ainsi entrer en tension avec les besoins de l'IA dans ses applications possibles en matière de renseignement.

À cet égard, deux difficultés ou questionnements particuliers peuvent être soulignés.

Tout d'abord, le développement de l'IA interroge la portée et la pertinence des règles de conservation des données en ce qu'elles se fondent sur la distinction entre les « renseignements collectés », données brutes recueillies, et les « transcriptions » ou « extractions », données travaillées. Or, l'utilisation de SIA dans les dispositifs de collecte de renseignement ou dans les outils de gestion des données peut brouiller ces distinctions. Les SIA reposant sur des techniques d'auto-apprentissage soulèvent à cet égard des questions nouvelles en créant une nouvelle catégorie de données, les données incrémentées dans le modèle lui-même. Les données brutes mises en entrée dans le SIA étant incorporées au système, la détermination d'une durée de conservation autre que la durée d'utilisation du SIA a moins de sens.

Ensuite, le développement de l'IA est susceptible de mettre à mal la pertinence des durées retenues au regard des difficultés d'exploitation qu'il génère pour les services. Il en va ainsi, par exemple,

des nouvelles possibilités de chiffrement et de cryptographie qui rendent plus ardue et chronophage l'analyse des données. C'est au demeurant cette considération qui a amené le législateur à introduire des délais de conservation dérogatoires pour les renseignements contenant des éléments de cyber-attaque ou chiffrés[50]. Une préoccupation similaire a également abouti à l'introduction en 2021 de durées de conservation des données plus longues pour permettre le développement, l'amélioration et la validation des dispositifs techniques de recueil et d'exploitation, le législateur ayant pris en compte les besoins en données nécessaires au développement des outils d'intelligence artificielle[51]. Cette dérogation s'inscrit dans la même optique que les réglementations, tel l'*AI Act* européen, qui prévoient la mise en place de « bacs à sable » réglementaires consistant à créer un cadre juridique spécifique pour le développement, la mise à l'essai et la validation de systèmes innovants.

Enfin, il faut relever que le cadre légal en vigueur est largement construit sur le principe d'une exploitation humaine du renseignement, par des personnes physiques, agents individuellement désignés et habilités, sans prendre en considération l'intervention de machines.

Outre l'appréhension de la donnée, l'essor des SIA questionne également certaines des distinctions et frontières essentielles fixées par la réglementation en vigueur.

Se pose tout d'abord la question de la détermination même des techniques de renseignement réglementées, alors que le livre VIII du code de la sécurité intérieure fonde le droit du renseignement sur une approche par technique de renseignement et non par opération ou par cible. Le développement des SIA amène en effet à s'interroger sur la possible émergence de nouvelles techniques réglementées en corrélation avec les progrès technologiques réalisés, évolution qui suppose au préalable de distinguer, parmi les systèmes présentant

50. Voir le I de l'article L. 822-2 du code de la sécurité intérieure.

51. Voir III de l'article L. 822-2 du code de la sécurité intérieure issu de l'article 10 de la loi 2021-998 du 30 juillet 2021, et rapport des sénateurs Marc-Philippe Daubresse et de Agnès Canayer, nº 694 du 16 juin 2021, sur le projet de loi.

un intérêt pour les surveillances, ceux qui doivent être érigés en techniques de renseignement de ceux qu'il n'y a lieu de regarder que comme de simples procédés incorporés à une technique visée au code de la sécurité intérieure ou à un outil d'exploitation.

L'essor de l'IA interroge également sur l'éclatement des législations et de la gouvernance dans les domaines du numérique et de la gestion de la donnée. Comme exposé ci-dessus, l'emploi des techniques d'IA est à la croisée de différentes réglementations et leur régulation fait intervenir plusieurs autorités ou entités de contrôle[52], soulevant la question de la cohérence des règles applicables. En matière de renseignement, les évolutions technologiques ont rapproché les moyens et procédés utilisés par les différents acteurs en matière de sécurité publique et favorisé un continuum des actions, rendant plus délicate la détermination de la frontière entre surveillance publique et surveillances secrète et plus aisées les possibilités de contournement de la législation la plus contraignante. Conjuguées à la révolution de la donnée, elles favorisent également la confusion entre le traitement des données et l'exploitation des résultats des surveillances.

2.2. … qui appellent une vigilance et un contrôle renforcés

Dans le cadre de la marge d'appréciation laissée aux États membres par la législation européenne sur l'IA, des pistes internes de régulation ont d'ores et déjà été formulées pour assurer un équilibre satisfaisant entre le développement d'un écosystème européen favorable à l'innovation technologique et le respect des droits et libertés fondamentaux.

L'une des préconisations les plus courantes consiste à privilégier, du moins dans un premier temps, un encadrement par le droit souple afin de rendre

52. Notamment, au niveau national, la CNIL, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) et la Direction interministérielle du numérique (DINUM).

plus aisée son adaptation aux évolutions, peu prévisibles, des technologies. L'utilisation des SIA dans des domaines très sensibles, notamment en matière de sécurité et de défense, pourrait toutefois faire l'objet d'une régulation nationale au moyen de réglementations sectorielles plus strictes.

Sans attendre une telle intervention normative, le développement de l'IA dans le domaine du renseignement appelle une évolution des modalités de contrôle. Ainsi, en l'absence d'encadrement spécifique, l'usage des SIA par les services amène les autorités de contrôle, parmi lesquelles tout particulièrement la CNCTR, à dégager, en s'appuyant sur le corpus juridique existant, les règles et principes à respecter pour que leur emploi soit respectueux des droits et libertés fondamentaux. Si un tel exercice reste usuel pour la plupart des organismes de contrôle, les principes directeurs de fonctionnement des SIA utilisés pour les opérations les plus sensibles de la chaîne du renseignement, tels l'exigence de pouvoir expliquer les traitements, la nécessité d'un contrôle humain de leurs résultats, ou encore l'impératif de robustesse des modèles déployés, dont la commission s'emploie d'ores et déjà à assurer le respect, mériteraient de recevoir une assise légale. Il en va de même de la supervision de l'usage des SIA par les services de renseignement, dont la reconnaissance comme l'une de ses missions à part entière de la CNCTR serait un gage de confiance pour les citoyens.

2.2.1. | Des garanties possibles en matière de renseignement

L'essor des SIA conforte en effet l'impératif de renforcement humain et technique des capacités de contrôle de la CNCTR[53] afin qu'elle soit en mesure, d'une part, de faire face à l'augmentation du volume des techniques de renseignement autorisées et des données recueillies par les services et, d'autre part, d'apprécier la robustesse comme l'acceptabilité des systèmes employés pour mettre en œuvre ces techniques et exploiter ces données.

53. Voir notamment 7ème rapport d'activité 2022 de la CNCTR, p. 56 et suivantes.

De la même manière, il rend plus cruciales encore les évolutions préconisées par la CNCTR en matière de centralisation des données recueillies et d'accès à distance[54] à ces données aux fins de contrôle, eu égard aux risques et enjeux précédemment évoqués.

Dans le contexte normatif actuel, il amène aussi au développement d'une nouvelle modalité du contrôle *ex ante* au travers de la formulation de lignes directrices ou de recommandations visant, dans l'imprécision ou le silence du code de la sécurité intérieure, à veiller à la compatibilité des technologies employées par les services avec des principes généraux posés par les textes.

Cette possibilité, qui peut s'inscrire dans les prérogatives générales de formulation de recommandations, observations et avis reconnues à la CNCTR par les articles L. 833-6, L. 833-10 et L. 833-11 du code de la sécurité intérieure, est un outil essentiel pour éviter que ne se développe l'usage par les services de « boites noires », à l'impact peu ou mal connu. Elle est de fait une voie permettant d'appliquer aux outils d'IA utilisés en matière de renseignement une régulation prudentielle relevant du même esprit que celle prévue pour les SIA à haut risque par la réglementation européenne, qui impose aux fournisseurs une certification des modèles et applications d'intelligence artificielle.

Dans une démarche analogue à celle fixée par l'*AI Act*, cet axe de contrôle consiste, au vu des caractéristiques des procédés et algorithmes proposés par les services et de la documentation technique transmise, à auditer ces outils et analyser leur impact sur les principes légaux et les droits fondamentaux, puis à recommander une doctrine d'emploi. Celle-ci s'attache tant à assurer le respect des règles générales posées par le code de la sécurité intérieure qu'à veiller à la prise en compte des principes nécessaires à la préservation des droits et libertés fondamentaux, tels l'impératif du contrôle humain sur les résultats des SIA ou le caractère individualisé de la surveillance domestique.

54. Voir point 3.1 du rapport d'activité.

Le succès de cette démarche impose de prévoir les modalités d'accès aux modèles et à leurs applications pour les agents en charge du contrôle et exige de ces derniers une expertise juridique et technique pointue pour comprendre les systèmes et en mesurer les enjeux. L'efficacité de ce nouvel axe de contrôle, qui s'inscrit pour la CNCTR dans une démarche d'appui et de régulation par le droit souple, suppose ainsi une meilleure transparence des services quant aux outils déployés.

LES PRINCIPES EUROPÉENS DE RÉGULATION DES SIA À HAUT RISQUE (*AI ACT*)

Des obligations fortes pour le fournisseur du système :

Le fournisseur doit en particulier :
– mettre en place des systèmes adéquats d'évaluation et d'atténuation des risques (identification et analyse de risques connus et prévisibles ; estimation et évaluation des risques potentiels, adoption de mesures appropriées de gestion des risques, etc.). ;
– assurer la gouvernance des données alimentant le système, en veillant à ce que les jeux de données de formation, de validation et de test soient pertinents, suffisamment représentatifs, exempts d'erreurs et complets, afin de minimiser les risques et les résultats discriminatoires ;
– fournir une documentation détaillée comportant toutes les informations nécessaires sur le système et son objet, pour permettre aux autorités d'évaluer sa conformité ;
– prévoir un contrôle humain, afin de minimiser les risques ;
– assumer un haut niveau de robustesse, de sécurité et de précision des modèles.

Un examen de conformité :

Avant la mise en service du SIA à haut risque, le fournisseur doit se soumettre à une procédure d'évaluation de la conformité du système aux obligations prévues par le règlement. Pour la plupart des SIA, l'évaluation est réalisée dans le cadre d'une procédure de contrôle interne, sans intervention d'un organisme extérieur. Pour les SIA les plus risqués, l'évaluation doit relever d'une autorité extérieure indépendante.

2.2.2. Au-delà du seul renseignement, l'enjeu d'une régulation cohérente de l'ensemble des techniques de surveillance

L'entrée en vigueur de la législation européenne sur l'IA et la mise en place des différents mécanismes de supervision qu'elle instaure imposera d'adopter une nouvelle gouvernance du numérique.

Eu égard à la place qu'occupent les données personnelles dans les problématiques relatives à l'IA, la fonction d'autorité de contrôle nationale responsable de la régulation des SIA pourrait incomber à la CNIL. Telle est notamment la préconisation de deux récentes missions d'information de la commission des lois constitutionnelles, de la législation et de l'administration de l'Assemblée nationale[55] et de la commission des affaires européennes du Sénat[56], conclusion qui rejoint l'avis de la CNIL elle-même et de ses homologues européens[57]. Au demeurant, on peut relever que, s'agissant des SIA des institutions de l'Union, la législation européenne confie le rôle de régulateur au Contrôleur européen de la protection des données.

Le rôle de régulation de marché qui serait ainsi confié à la CNIL n'épuiserait toutefois pas les besoins de contrôle des SIA. Hors du champ de la législation européenne, les SIA utilisés en matière de sécurité nationale et de défense mériteraient une régulation et un encadrement spécifiques visant à concilier la préservation des droits et libertés individuels et l'impératif de discrétion, voire de secret lorsque sont en cause des informations classées au titre du secret de la défense nationale, qu'exige l'efficacité de l'action publique dans ces domaines.

55. Voir le rapport d'information au nom de la commission des affaires la commission des lois constitutionnelles, de la législation et de l'administration sur les défis de l'intelligence artificielle générative en matière de protection des données personnelles et d'utilisation du contenu généré, de MM. Pradal et Rambaud enregistré le 14 février 2024.

56. Voir le rapport d'information au nom de la commission des affaires européennes relatif à la proposition de législation européenne sur l'intelligence artificielle, de M. André Gattolin, Mme Catherine Morin-Desailly, M. Cyril Pellevat et Mme Elsa Schalck enregistré le 30 mars 2023.

57. Avis du 18 juin 2021 sur la proposition de règlement de la Commission européenne sur l'IA.

Les différentes technologies concourant à la sécurité nationale et la défense, qui recouvrent des pratiques courantes, telle la vidéo-surveillance des lieux publics, des méthodes plus récentes, comme la captation d'images par drones ou caméras embarqués, jusqu'aux procédés particulièrement intrusifs que représentent les technologies de reconnaissance faciale ou certaines techniques de renseignement secrètes comme le recueil de données informatiques, relèvent aujourd'hui de contrôles éclatés, réalisés par des autorités de nature diverse, sans supervision générale. Pourtant, les politiques publiques de sécurité et de renseignement se traduisent dans ce domaine par un continuum d'actions et se rapprochent par les techniques employées.

Une supervision étroite et un contrôle coordonné de l'usage de ces nouvelles technologies par les forces de sécurité, garantissant un emploi proportionné aux besoins de la sécurité collective sans instrumentation pour une surveillance de masse, seraient un gage de leur efficacité et de leur acceptabilité sociale.

Éclairage 2. L'usage responsable des capacités commerciales de cyber-intrusion : une perspective diplomatique

Contribution de M. Henri VERDIER, ambassadeur pour le numérique, et de M. Léonard ROLLAND, sous-directeur de la cyber-sécurité à la direction des affaires stratégiques, de sécurité et du désarmement au ministère de l'Europe et des affaires étrangères

Depuis un quart de siècle, en réponse aux défis induits par l'apparition d'un nouvel espace de conflictualité numérique, les États négocient à l'ONU, comme au sein de formats diplomatiques *ad hoc*, les paramètres de ce qu'ils estiment être un « comportement responsable » dans le cyberespace, et notamment un « usage responsable » des capacités cyber.

Certaines de ces capacités, comme les outils de cyber-intrusion, peuvent être utilisées légitimement par les services de renseignement et les forces de sécurité intérieure dans le respect d'un cadre légal strict, pour des enquêtes administratives ou judiciaires sous le contrôle de la CNCTR ou d'un magistrat. En parallèle de ces usages légitimes, s'est développé depuis quelques années un marché des capacités d'intrusion, porté par des entreprises privées vendant aux plus offrants. Ces capacités sont ensuite susceptibles d'être utilisées dans des conditions ne garantissant ni le respect des droits de l'Homme, ni la stabilité et la sécurité du cyberespace.

Face aux risques nés de la prolifération et de l'usage irresponsable des outils numériques offensifs, il est donc nécessaire d'adopter une approche et une gouvernance à même de définir les rôles et les responsabilités

respectifs des États et du secteur privé. C'est dans cet esprit que l'Appel de Paris lancé par le Président de la République en 2018, et soutenu par un grand nombre d'États et d'entreprises, a souhaité inscrire ce sujet à l'ordre du jour de nos discussions internationales. L'Appel affirmait alors que la lutte contre la prolifération des logiciels malveillants et les pratiques informatiques destinées à nuire constituait un principe à part entière pour assurer la confiance et la sécurité dans le cyberespace.

Ce phénomène de prolifération cyber par des acteurs privés fait l'objet depuis peu d'une initiative diplomatique *ad hoc*. En février 2024, la France et le Royaume-Uni ont en effet conjointement lancé le Processus de Pall Mall, un processus diplomatique de long terme dont l'objet est la lutte contre la prolifération et l'usage irresponsable de capacités de cyber-intrusion disponibles sur le marché. Au cœur de nos travaux diplomatiques, la notion d'« usage responsable » de telles capacités par les États qui devra faire l'objet d'un important travail de définition. De même, l'initiative a vocation à recenser et promouvoir les « bonnes pratiques » en matière de contrôle de cet usage. Dans ce cadre, la France sera naturellement amenée à promouvoir son approche et ses pratiques nationales, parmi lesquelles le travail de contrôle exercé par la CNCTR.

Le défi de l'émergence d'un marché de la cyber-intrusion

Dans une déclaration adoptée à l'occasion du lancement du processus de Pall Mall en février 2024, une coalition composée d'États, d'entreprises, et de représentants de la société civile soulignait à propos du marché de la cyber-intrusion que « *ce marché en croissance, avec ses effets transformationnels sur le paysage cyber, élargit considérablement le groupe potentiel d'acteurs étatiques et non étatiques ayant accès à des capacités d'intrusion cyber de nature commerciale, accroît les risques d'usages malveillants et irresponsables et rend plus difficiles l'atténuation des menaces qui en découlent et la protection contre celles-ci.* » Avant de poursuivre en soulignant le défi multiple que ce phénomène pose : « *ces menaces, qui pèsent notamment sur la stabilité*

cyber, les droits de l'Homme, la sécurité nationale et la sécurité numérique dans son ensemble, sont appelées à s'intensifier durant les années à venir ».

Dans son Panorama de la menace 2023, publié également en février 2024, l'Agence nationale de sécurité des systèmes d'information (ANSSI) confirme le constat : « *si ces capacités sont historiquement développées par des États possédant des capacités offensives avancées, l'essor du marché privé de la surveillance se confirme : certaines entreprises fournissent des codes malveillants très perfectionnés à des acteurs publics, mais également à des entreprises et à des particuliers aux intentions malveillantes. La prolifération d'outils offensifs commerciaux contribue de manière significative à l'augmentation générale du niveau de menace* ».

L'irruption massive de capacités d'intrusion de nature commerciale est susceptible d'entraîner une transformation des pratiques des États. À l'échelle internationale, on observe déjà de façon très manifeste des excès dans l'usage de ces capacités, ce qui fait régulièrement l'objet de publications diverses ; il convient dès lors d'en définir un cadre d'usage responsable.

La nécessaire définition d'un cadre d'usage responsable : le modèle français

L'industrie de la cyber-intrusion répond à des besoins divers et les produits qui en sont issus ont souvent une nature duale. Ils peuvent ainsi être utilisés à des fins de cybersécurité (test d'intrusion pour vérifier la robustesse d'un système informatique par exemple), à des fins de sécurité nationale, mais ils peuvent aussi être détournés. Par exemple, un logiciel de captation de données qui jouerait un rôle vital dans une investigation anti-terroriste ou en matière de lutte contre la criminalité organisée peut également être utilisé à des fins de surveillance d'opposants politiques et de journalistes dans des conditions contraires au respect de l'État de droit. De cette complexité découle la nécessité d'éviter toute approche simpliste, de type prohibition, pour s'intéresser à la notion d'usage responsable et

aux mécanismes de contrôle associés. C'est pourquoi le Processus de Pall Mall en a fait, – avec la question du façonnement du marché lui-même – l'un de ses axes de travail.

S'agissant des mécanismes de contrôle de l'usage, l'approche du Processus de Pall Mall se veut empirique et a vocation à débuter par un parangonnage des pratiques actuelles. La France, où les grands équilibres du droit du renseignement sont exclusivement définis par le législateur national, sous le contrôle du Conseil constitutionnel, peut valoriser son modèle qui subordonne l'utilisation des capacités attentatoires à la vie privée à l'autorisation d'un magistrat pour les enquêtes judiciaires, et à l'obtention obligatoire et préalable de l'avis d'une autorité administrative indépendante pour les enquêtes administratives. Dans ce cadre, la CNCTR effectue un contrôle de légalité et de proportionnalité de la demande. Si son avis n'est pas suivi par le Gouvernement – ce qui n'est jamais arrivé jusqu'à présent – le juge administratif suprême (Conseil d'État) est immédiatement saisi.

Parmi les autres moyens dont disposent les États pour contrôler la prolifération et l'usage de capacités de cyber-intrusion, le contrôle à l'export est souvent cité. De fait, les logiciels d'intrusion sont couverts depuis 2013 par l'Arrangement de Wassenaar, un régime multilatéral de contrôle des exportations en matière d'armes conventionnelles et de biens et technologies à double usage dont la France fait partie. Moins connus sont les mécanismes de contrôle à l'importation, auxquels contribue par exemple en France le dispositif « R. 226 » du nom de l'article du code pénal qui en constitue la base juridique[58]. Ce dispositif interministériel au sein duquel siège la CNCTR permet ainsi d'exercer un contrôle sur les matériels importés susceptibles de porter atteinte au secret des correspondances, dont les logiciels de captation de données par exemple.

58. « 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 délivrée par le Premier ministre, après avis de la commission mentionnée à l'article R. 226-2. »

Un effort multi-acteurs vers une meilleure régulation

Alors qu'une conférence de suivi du Processus de Pall Mall sera organisée en France en 2025, se dessinent progressivement les prochaines étapes de l'initiative. Parmi elles, la volonté d'échanger entre parties prenantes sur les meilleures pratiques de la part des États, des entreprises ou encore de la société civile pour contribuer à lutter contre la prolifération et l'usage irresponsable des capacités de cyber-intrusion disponibles sur le marché.

À terme, l'ambition de ce processus de type « *soft law* » est d'aboutir à un corpus de règles de bonne conduite, à la manière de celui régissant les activités des entreprises de services de sécurité et de défense (ESSD), aussi appelé Document de Montreux, adopté en 2008. Nul doute que la question du contrôle sera un élément clé de cet effort de régulation internationale.

Annexes

1. Évolution de la composition du collège de la CNCTR au cours de l'année 2023

La composition du collège de la CNCTR a connu un renouvellement concernant un de ses membres en 2023.

Le 6 novembre 2023, M. Jérôme DARRAS, sénateur du Pas-de-Calais, a été nommé membre de la CNCTR par le président du Sénat. Il a succédé à M. Yannick VAUGRENARD, dont le mandat était parvenu à son terme.

À la fin de l'année 2023, le collège de la CNCTR était composé des **neuf membres** suivants :

- **M. Serge LASVIGNES**, conseiller d'État honoraire, président ;
- **M^me^ Chantal DESEYNE**, sénateur d'Eure-et-Loir ;
- **M. Jérôme DARRAS**, sénateur de la Loire-Atlantique ;
- **M^me^ Michèle TABAROT**, députée des Alpes-Maritimes ;
- **M. Yannick CHENEVARD**, député du Var ;
- **M^me^ Françoise SICHLER-GHESTIN**, conseillère d'État honoraire ;
- **M^me^ Solange MORACCHINI**, avocate générale honoraire à la Cour de cassation ;
- **M. Gérard POIROTTE**, conseiller honoraire à la Cour de cassation ;
- **M. Philippe DISTLER**, personnalité qualifiée en matière de communications électroniques.

Les modalités de désignation ou de nomination des membres sont fixées par l'article L. 831-1 du code de la sécurité intérieure. 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 des dispositions de l'article L. 831-2 du code de la sécurité intérieure, la formation plénière de la commission comprend l'ensemble de ses membres et la formation restreinte est composée de tous les membres qui ne sont pas parlementaires.

2. Les moyens de la CNCTR

2.1. Les ressources humaines

Depuis le 1er novembre 2023, sur les 9 membres que compte le collège de la commission, quatre exercent désormais leurs fonctions à temps plein. Il s'agit du président de la CNCTR, des deux membres honoraires de la Cour de cassation et de la personnalité qualifiée.

Ce renforcement de la présence quotidienne des membres ayant la qualité de magistrat[1] a été rendu nécessaire par l'intensification de l'activité de contrôle *a posteriori* de la commission[2] ainsi que par l'augmentation du nombre de demandes de techniques dont elle est saisie. Les dispositions du code de la sécurité intérieure imposent en effet un délai de vingt-quatre heures à la CNCTR pour rendre ses avis sur les demandes dont l'examen en formation collégiale n'est pas requis ; ces avis ne pouvant être rendus que par les membres ayant la qualité de magistrat.

Lorsque la demande dont est saisie la commission 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[3]. En conséquence, ces formations collégiales se réunissent sauf exception trois fois par semaine, les lundis, mercredis et vendredis, toute l'année, ce qui représente plus de 140 séances par an, auxquelles s'ajoutent chaque mois une réunion solennelle de l'ensemble de ses membres en une formation plénière. Ces réunions plénières

1. Membres mentionnés aux 2° et 3° de l'article L. 831-1 du code de la sécurité intérieure.
2. Voir le point 2.1.1 du présent rapport.
3. Voir les dispositions de l'article L. 821-3 du code de la sécurité intérieure.

mensuelles débutent en général par une audition (coordonnateur national du renseignement et de la lutte contre le terrorisme, chefs de service, directeur du GIC, directeur de cabinet des ministres dont relèvent les services…), donnent lieu à l'examen des projets de délibérations les plus importantes et comportent également 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 dans les locaux de la commission afin d'éclairer le collège sur des sujets d'ordre technique ou juridique.

Pour son fonctionnement, le collège de la CNCTR s'appuie sur une équipe comptant, au 31 décembre 2023, 20 agents : une secrétaire générale, un conseiller placé auprès du président, 14 chargés de mission[4] et 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 conducteur investi par ailleurs des fonctions d'officier de sécurité adjoint).

Les chargés de mission de la CNCTR sont, pour l'essentiel, des agents de catégorie A+ et assimilés, dont le rôle principal est d'instruire les demandes de mise en œuvre de techniques de renseignement et de conduire les contrôles *a posteriori*, sous la supervision d'un membre de la commission.

Ils sont, de manière à peu près égale, soit des agents publics détachés (magistrats judiciaires et administratifs, commissaire de police, ingénieur de l'armement), soit des agents contractuels (ingénieurs notamment). S'y ajoute un officier supérieur de gendarmerie mis à disposition de la CNCTR contre remboursement de sa rémunération. Eu égard aux missions d'instruction et de contrôle qui leur sont confiées, les agents

4. Dont un conseiller technique et un coordonnateur des activités de contrôle *a posteriori*.

de la commission sont essentiellement recrutés pour leurs compétences juridiques ou techniques.

Le personnel du secrétariat est, quant à lui, composé de deux fonctionnaires titulaires et de deux agents contractuels.

L'équipe de la CNCTR se compose de 55 % de femmes et 45 % d'hommes. 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 sont inscrits au budget général de l'État (mission « Direction de l'action du Gouvernement », programme n° 308 « Protection des droits et libertés », action n° 12 « Commission nationale de contrôle des techniques de renseignement »).

La loi de finances initiale pour 2023[5] a attribué à la CNCTR des montants d'un peu plus de 2,7 millions d'euros pour ses dépenses de personnel (T2) et d'un peu plus de 400 000 euros pour ses dépenses de fonctionnement.

Conformément aux créations de postes qui ont été accordées à la commission pour les années 2022, 2023 et 2024[6], il a pu être procédé à deux recrutements en 2023 (deux chargés de mission au profil généraliste) ainsi qu'à la transformation en emploi à temps plein du poste d'un membre du collège. Le renforcement du pôle technique est plus compliqué à concrétiser. Deux recrutements sont ainsi toujours envisagés pour l'année 2024.

5. Loi n° 2022-1726 du 30 décembre 2022 de finances pour 2023.

6. Voir sur ce point le 7ème rapport d'activité 2022 de la CNCTR, p. 64 et suivantes et p. 134.

Le contexte, décrit dans le corps du rapport d'activité, l'augmentation du nombre des demandes de techniques, la nécessité de garantir l'efficience de la capacité de contrôle *a posteriori* tant d'un point de vue quantitatif que qualitatif, enfin la hausse du nombre de réclamations, font que la poursuite de cette tendance haussière à la fois des effectifs et du budget de fonctionnement de la commission apparaît indispensable au bon accomplissement des missions qui lui ont été confiées par le législateur. Au-delà, à moyen terme, se posera la question d'un nouveau dimensionnement de la commission de manière à atteindre une taille critique lui permettant de sécuriser les différentes fonctions support.

3. Les relations extérieures de la CNCTR

Au cours de l'année 2023, la commission a poursuivi son dialogue fructueux avec ses partenaires institutionnels, le monde universitaire mais également ses homologues étrangers. Elle a aussi assuré un certain nombre de formations au bénéfice de diverses entités publiques. Ces nombreux échanges et interactions permettent à la commission de partager son point de vue sur le cadre légal applicable au renseignement et de porter le cas échéant ses attentes en la matière. Ils contribuent également à diffuser la connaissance de ce cadre légal, à améliorer les pratiques et à bénéficier de l'expérience des homologues étrangers de la commission en la matière.

3.1. Un colloque co-organisé avec la DPR

En mai 2023, la CNCTR, a ainsi co-organisé avec la Délégation parlementaire au renseignement (DPR), un **colloque consacré au contrôle de la politique publique du renseignement**. Ouvert par la présidente

de l'Assemblée nationale, ce colloque, qui s'est tenu à l'Hôtel de Lassay, a réuni des membres du Parlement, des magistrats, des représentants des services de renseignement et d'autorités administratives indépendantes, ainsi que des universitaires. Il a été l'occasion de débattre des modalités d'une mobilisation efficace du renseignement dans un monde plus lourd de menaces, tout en assurant une protection effective des libertés et de la vie privée face au renforcement des moyens des services et au développement rapide des technologies de surveillance.

3.2. Un dialogue entretenu avec le Parlement

S'agissant plus particulièrement du **dialogue institutionnel entretenu avec le Parlement**, le président de la CNCTR a été auditionné à cinq reprises par le Sénat au cours de l'année 2023 :

- en mai, il a été entendu par M. Philippe Bas, rapporteur de la **proposition de la loi relative à la reconnaissance biométrique dans l'espace public**[7] pour la commission des lois. Il a notamment été interrogé sur les possibilités de recourir à des technologies relevant de l'intelligence artificielle pour faciliter le traitement des données recueillies dans le cadre de techniques de renseignement ou fiabiliser les résultats des analyses menées par les services ainsi que sur les modalités d'encadrement d'une éventuelle expérimentation de la reconnaissance biométrique dans l'espace public ;

- en juin, il a été auditionné par M. Christian Cambon, rapporteur pour la commission des affaires étrangères, de la défense et des forces armées, sur le projet de **loi programmation militaire pour les années 2024 à 2030** qui a conduit à la loi n° 2023-703 du 1er août 2023 ;

- en juillet, il a été reçu par la **mission d'information sur les modalités d'investigation recourant aux données de connexion dans le**

7. Voir le dossier législatif sur le site du Sénat : https://www.senat.fr/dossier-legislatif/ppl22-505.html.

cadre des enquêtes pénales[8], et interrogé sur le fonctionnement du régime juridique spécial encadrant l'accès à ces données en matière de police administrative, ainsi que sur les modifications apportées par la *loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement* pour mettre en conformité la législation française relative au renseignement avec le droit de l'Union européenne régissant la conservation par les opérateurs de communications électroniques des données de leurs abonnés ;

- et en octobre 2023, il a été auditionné par la rapporteure pour la commission des lois dans la procédure d'avis budgétaire portant sur la mission «Direction de l'action du gouvernement» lors de l'examen au Sénat du projet de loi de finances pour l'année 2024.

Par ailleurs, il a été entendu à deux reprises à l'Assemblée nationale :

- en juillet, il a été interrogé par les rapporteurs de la **mission d'information sur l'intelligence artificielle générative**[9] et a livré ses réflexions sur les perspectives ouvertes par le développement de l'intelligence artificielle en matière de renseignement, et ses conséquences éventuelles pour l'activité de contrôle de la commission, en mettant l'accent sur l'importance d'une étroite supervision humaine, dès lors que les outils concernés se perfectionnent et leurs domaines d'application se diversifient[10] ;

- en juillet également, il a été auditionné par la **commission d'enquête sur la structuration, le financement, les moyens et les modalités d'action des groupuscules auteurs de violences à l'occasion des manifestations et rassemblements intervenus entre le 16 mars et le 3 mai 2023 ainsi que sur le déroulement de ces manifestations et rassemblements**[11]. Il a notamment été entendu sur le caractère suffisamment exhaustif du cadre juridique actuel s'agissant de la prévention des violences collectives.

8. Voir : *https://www.senat.fr/notice-rapport/2023/r23-110-notice.html*.

9. Voir : *https://www.assemblee-nationale.fr/dyn/16/organes/commissions-permanentes/lois/missions-d-information-de-la-commission-des-lois/intelligence-artificielle-protection-donnees-personnelles*.

10. Voir également sur ce point la partie « Éclairages » du présent rapport, ci-dessus.

11. Voir : *https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cegrvimani/l16cegrvimani2223021_compte-rendu#*

3.3. Les autres interlocuteurs institutionnels de la commission

Le président de la CNCTR a par ailleurs été auditionné en janvier 2023 par les membres de la **commission du Parlement européen spécialement chargée d'enquêter sur l'utilisation par certains États du logiciel de surveillance dit « Pegasus »**[12], afin de leur présenter le cadre légal régissant en France l'utilisation des techniques de renseignement. Il en a décrit les principes fondateurs et témoigné de la façon dont il fonctionne, en rendant compte notamment des limites qu'il impose aux services de renseignement ainsi que des caractéristiques originales du dispositif prévu en France pour le contrôle de leur action. Il a également formulé des pistes de réflexion pour l'encadrement de ce type d'outils de surveillance par le législateur national.

La commission a également été entendue à trois reprises par la **Cour des comptes** dans le cadre de sa mission de contrôle des comptes et de la gestion des services de renseignement.

3.4. Les relations internationales de la commission

S'agissant des relations internationales, la CNCTR a continué à entretenir un dialogue avec ses homologues étrangers dans le cadre de réunions bilatérales mais également multilatérales.

Une délégation de la commission a ainsi participé les 9 et 10 novembre 2023, à Oslo, à la **Conférence européenne de contrôle du renseignement**, qui réunit chaque année les autorités nationales de contrôle appartenant à de nombreux pays d'Europe.

12. Voir : *https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/OJ/2023/01-09/1269403FR.pdf*.

Les échanges ont notamment porté sur l'utilisation des données publiques, les modalités d'un contrôle efficace, la jurisprudence de la Cour européenne des droits de l'homme ainsi que la responsabilité des organes de contrôle et les modalités de publicité de leur activité.

Enfin, fin novembre 2023, la CNCTR a contribué à la sixième édition du **Forum international du contrôle du renseignement** (« *International Intelligence oversight Forum* ») qui s'est déroulée cette année à Washington DC et qui a notamment abordé la question de la nécessité et de la proportionnalité de la surveillance.

3.5. Les formations auxquelles la commission a contribué

Au cours de l'année écoulée, la commission a également poursuivi sa participation 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 2023 devant les auditeurs de l'**Académie du renseignement**.

Par ailleurs, elle a contribué à deux sessions de formations dispensées par l'**École nationale de la magistrature** et est intervenue à deux reprises au **Centre des hautes études militaires** (CHEM).

3.6. La communication à l'égard du grand public

Enfin, de façon plus générale et à destination du grand public, outre la publication de son rapport annuel d'activité, la CNCTR a poursuivi son effort de mise à disposition d'informations aussi détaillées que le permet le secret de la défense nationale sur sa mission et l'exercice de son action de contrôle.

À cet égard, dans le prolongement de la refonte de son site Internet[13] intervenu au cours de l'année 2023, la commission a enrichi les ressources qui y sont accessibles en particulier par de nombreuses fiches thématiques sur les finalités permettant de recourir aux techniques de renseignement prévues par le code de la sécurité intérieure, la teneur de ces techniques et leur périmètre d'application.

13. *https://www.cnctr.fr/*

4. Délibération n° 2/2023 du 16 novembre 2023 portant adoption du règlement intérieur de la Commission nationale de contrôle des techniques de renseignement

Article 1er

Le nouveau règlement intérieur de la Commission nationale de contrôle des techniques de renseignement, dans la rédaction figurant en annexe, est adopté.

Article 2

La délibération n° 2/2017 du 23 mars 2017 portant adoption du règlement intérieur est abrogée.

Article 3

La secrétaire générale de la Commission nationale de contrôle des techniques de renseignement est chargée de l'exécution de la présente décision qui sera publiée au Journal officiel de la République française.

Annexe

Règlement intérieur de la Commission nationale de contrôle des techniques de renseignement adopté par la commission réunie en formation plénière le 16 novembre 2023

Titre Ier - Règles déontologiques applicables aux membres et agents de la Commission nationale de contrôle des techniques de renseignement

Article 1er – Indépendance

Les membres et les agents de la Commission nationale de contrôle des techniques de renseignement, ci-après dénommée « la commission », s'abstiennent de tout comportement de nature à faire naître un doute sur l'indépendance de l'institution.

Ils respectent une obligation générale de loyauté à l'égard de l'institution.

Ils ne sollicitent, ni ne reçoivent aucune instruction d'une quelconque autorité.

Article 2 – Prévention des conflits d'intérêts

I. - Lorsque les membres et les agents de la commission estiment que leur participation à une délibération ou à un contrôle les placerait en situation de conflit d'intérêts ou que pour toute autre raison quelconque, de leur propre fait ou de celui d'autrui, leur indépendance n'est pas ou peut ne pas apparaître assurée, ils en informent le président dès qu'ils ont connaissance de cette situation et, au plus tard, au début de la délibération ou du contrôle concerné. Ils s'abstiennent de prendre part à la délibération ou au contrôle concerné et d'émettre un avis. Le président informe les autres membres de la commission sans délai des conflits d'intérêts dont il a connaissance en vertu de l'alinéa précédent ou de ceux qui le concernent.

II. - Les membres et le secrétaire général adressent au président de la commission copie de la déclaration d'intérêts prévue au 6° de l'article 11 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique. La déclaration d'intérêts de chaque membre est mise, de façon permanente, à la disposition des autres membres dans les locaux de la commission. Le président restitue aux membres et au secrétaire général leur déclaration d'intérêts dans un délai de six mois suivant la fin de leurs fonctions au sein de la commission.

Article 3 – Secret de la défense nationale, secret professionnel, discrétion professionnelle

Les membres et les agents de la commission observent le secret de la défense nationale dans les conditions prévues par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale ainsi que le secret professionnel et le devoir de discrétion professionnelle auxquels ils sont tenus par la loi.

Ces obligations se perpétuent après le terme du mandat de membre ou des fonctions d'agent de la commission.

Le secret de la défense nationale n'est pas opposable aux membres et aux agents de la commission entre eux. Ils se doivent mutuellement toute l'information utile au bon accomplissement de leurs missions.

Le partage du secret de la défense nationale avec un service ou un agent extérieur à la commission pour le traitement d'un dossier n'autorise pas la méconnaissance du secret couvrant une autre affaire.

Aucune affaire particulière ou générale couverte par le secret de la défense nationale ne peut être évoquée avec un service ou un agent qui n'a pas besoin d'en connaître ou n'y est pas habilité.

Article 4 - Impartialité

Les demandes soumises pour avis à la commission sont examinées avec impartialité et neutralité.

Investis d'une mission de contrôle des services autorisés à mettre en œuvre des techniques de renseignement, les membres et les agents de la commission ne peuvent avoir avec les agents de ces services que des relations conciliables avec l'exercice d'un tel contrôle.

Article 5 – Attitude durant les contrôles

Lors des contrôles, les membres et les agents de la commission se soumettent aux règles de sécurité applicables dans les services de renseignement concernés.

Ils ne se départissent jamais de la courtoisie requise.

Ils demandent aux responsables des lieux ainsi qu'aux agents exploitants de leur permettre l'accès aux données qui leur sont utiles et de leur fournir les documents nécessaires à l'accomplissement du contrôle. Ils consignent avec précision tout refus d'accès aux données, accidentel ou délibéré, et, plus généralement, tout refus de coopération qui risquerait de compromettre la conduite de leur mission.

Ils se gardent de tout jugement pendant le déroulement de la visite. Ils se bornent à recueillir les informations qui leur sont utiles, à établir leur véracité et à poser les questions requises par leur compréhension.

Ils veillent à ce que les questions qu'ils posent soient en lien direct avec les attributions de la commission. Ils précisent en tant que de besoin en quoi leurs demandes relèvent de ces attributions.

Dans leur rapport, ils veillent en toute objectivité à faire la part des faits établis et celle des hypothèses et mettent en lumière les considérations qui leur paraissent mériter un examen par les membres de la commission.

Article 6

Toute difficulté rencontrée par les membres et les agents de la commission dans l'exercice de leurs missions est portée à la connaissance du président, qui peut inviter la formation restreinte ou plénière de la commission à en débattre.

Article 7 – Suspension du mandat, fin des fonctions ou démission d'un membre

La formation plénière de la commission délibère sur la suspension du mandat, la fin des fonctions ou la démission d'un membre pour l'un des motifs prévus à l'article 6 de la n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.

La délibération se déroule une semaine au moins après que l'intéressé a été mis en mesure de présenter des observations écrites ou, à sa demande, d'être entendu par la formation plénière. Le vote a lieu à bulletin secret hors la présence de l'intéressé.

Article 8 – Engagement sur l'honneur

Lors de leur prise de fonction, les membres et les agents de la commission attestent sur l'honneur du fait qu'ils s'engagent à respecter les dispositions du présent règlement intérieur.

Titre II - Organisation et fonctionnement de la commission

Chapitre Ier - Formations plénière et restreinte

Article 9 - Calendrier des formations plénière et restreinte et ordre du jour

Les formations plénière et restreinte fixent le calendrier de leurs réunions. Elles sont en outre réunies en tant que de besoin, à l'initiative du président.

Dans le cas prévu à l'article L. 821-7 du code de la sécurité intérieure, le président prend les dispositions nécessaires pour réunir la formation plénière dans les meilleurs délais.

Le président fixe l'ordre du jour des réunions en formations plénière et restreinte de la commission. Les membres de la commission peuvent demander l'inscription d'une question à cet ordre du jour.

Les documents utiles sont mis à la disposition des membres dans les locaux de la commission au plus tard vingt-quatre heures avant la séance.

Par dérogation au précédent alinéa, lorsque la commission est saisie afin de rendre un avis sur une demande de mise en œuvre de l'une des techniques de recueil de renseignement mentionnées aux chapitres I à IV du titre V du livre VIII du code de la sécurité intérieure, les documents utiles sont mis à la disposition des membres de la commission dans les meilleurs délais.

Article 10 – Présidence des formations plénière et restreinte

Les formations plénière et restreinte de la commission sont présidées par son président qui dirige les débats.

En cas d'absence, d'empêchement ou de déport du président, ou si le poste de président devient vacant pour quelque cause que ce soit, la présidence des formations plénière et restreinte est assurée par

le membre de la commission le plus ancien parmi les membres mentionnés aux 2° et 3° de l'article L. 831-1 du code de la sécurité intérieure. En cas de concours dans l'ancienneté entre plusieurs de ces membres, la présidence est exercée par le membre le plus âgé parmi ceux-ci.

Article 11 – Avis et délibérations de la commission

I. - Les formations plénière et restreinte de la commission statuent à la majorité des membres présents ou participant à la délibération, le président ayant voix prépondérante en cas de partage égal des voix.
En tant que de besoin, le président peut décider de recourir aux formes de délibération à distance prévues par l'ordonnance n° 2014-1329 du 6 novembre 2014 relative aux délibérations à distance des instances administratives à caractère collégial, dès lors que l'identification des participants, la confidentialité des débats et la protection du secret de la défense nationale sont assurées.
Sauf décision contraire du président, le secrétaire général et les agents de la commission assistent aux séances des formations plénière et restreinte.

II. - Le secrétaire général de la commission ou, en cas d'absence ou d'empêchement, l'agent de la commission désigné par le président, assure le secrétariat des séances des formations plénière et restreinte et en établit le procès-verbal.
Lorsque la commission est saisie afin de rendre un avis sur une demande de mise en œuvre de l'une des techniques de recueil de renseignement mentionnées aux chapitres I à IV du titre V du livre VIII du code de la sécurité intérieure, l'indication de la formation ayant examiné la demande, des membres présents et du sens de la décision rendue, portée sur la fiche d'instruction de la demande, peut tenir lieu de procès-verbal.
Les procès-verbaux, les avis et les délibérations de la commission, ainsi que les suites données à ces avis par le Premier ministre, sont tenus à la disposition des membres dans les locaux de la commission.

Article 12 - Doctrine

La formation plénière ou restreinte débat des principes régissant les avis rendus par la commission sur les demandes qui lui sont soumises ainsi que ses contrôles effectués sur la mise en œuvre des techniques de renseignement.

Article 13 – Contrôles

En concertation avec les membres de la commission, le président arrête le programme des visites de contrôle et les conditions dans lesquelles ces visites sont organisées. Il peut aussi décider de contrôles impromptus.

Les contrôles peuvent également être réalisés à distance.

Les résultats des contrôles et les suites données par les services concernés sont portés à la connaissance des formations plénière ou restreinte de la commission.

Article 14 – Suites données aux avis de la commission

I. – Lorsque l'autorisation mentionnée à l'article L. 821-1 du code de la sécurité intérieure est délivrée par le Premier ministre après un avis défavorable de la commission, le président de la commission ou, à défaut, l'un des membres de la commission, mentionnés aux 2° et 3° de l'article L. 831-1 du même code, saisit immédiatement le Conseil d'État et informe la formation plénière dans les meilleurs délais.

II. - La formation plénière est informée des recommandations adressées au Premier ministre, tendant à ce que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits, en application des articles L. 833-6 ou L. 854-9 du code de la sécurité intérieure. Elle débat des suites données par le Premier ministre à ces recommandations.

III. - La formation plénière décide des observations qu'elle juge utile d'adresser au Premier ministre en application de l'article L. 833-10 du code de la sécurité intérieure.

Article 15 – Demandes d'avis en application de l'article L. 833-11 du code de la sécurité intérieure

La formation plénière débat de la réponse qui doit être apportée aux demandes d'avis que peuvent, en application de l'article L. 833-11 du code de la sécurité intérieure, adresser à la commission le Premier ministre, le président de l'Assemblée nationale, le président du Sénat et la délégation parlementaire au renseignement.

Chapitre II - Organisation de la commission et traitement des demandes

Article 16

Les agents de la commission, sont placés sous l'autorité du président. Ils assistent les membres de la commission dans la conduite de leurs missions.

Le secrétaire général anime et coordonne leur action.

Article 17

Le président fixe, en concertation avec les membres et les agents de la commission, les conditions dans lesquelles sont rendus les avis sur les demandes de mise en œuvre des techniques de recueil de renseignement mentionnées aux chapitres I à IV du titre V du livre VIII du code de la sécurité intérieure soumises à celle-ci.

Le président veille à ce que les délais impartis à la commission pour émettre ses avis soient respectés.

Article 18

Toutes les demandes soumises à la commission sont examinées à la lumière des informations communiquées, qui sont interprétées strictement, sans altération ni omission.

Lorsque toutes les informations nécessaires à l'examen de la demande n'ont pas été communiquées, la commission invite le service à l'origine de la demande à lui transmettre des informations complémentaires dans les meilleurs délais.

Le délai légal d'examen court à compter du moment où la commission estime que la demande est complète.

Article 19

Toute question nouvelle ou toute difficulté sérieuse est, à l'initiative du président ou de l'un des membres de la commission, soumise, selon le cas, à la formation plénière ou à la formation restreinte de la commission.

Chapitre III - Rapport public, communication et relations extérieures

Article 20

Dans ses relations institutionnelles, la commission est représentée par le président, qui rend compte à la formation plénière.

La communication publique de la commission est assurée par le président, en concertation avec les membres.

Les agents de la commission ne peuvent s'exprimer au nom de l'institution, sauf mandat exprès du président.

Article 21

Le rapport public d'activité, débattu et approuvé en formation plénière, est remis par le président au Président de la République, au Premier ministre et aux présidents des deux assemblées.

Le président invite les parlementaires membres de la commission à l'accompagner lors de la visite qu'il rend au président de l'assemblée dans laquelle ils siègent.

Article 22

Le président, en concertation avec les membres et les agents de la commission, prend toutes dispositions pour mener les échanges utiles dans les cadres européen et international et promouvoir le modèle français de contrôle des techniques de renseignement.

Crédits photographiques : Damien Carles / Matignon, Assemblée nationale, Sénat.

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

Maquette et impression : DSAF / DPSG / BAEC / Section Édition – 25 juin 2024 - ISSN 2966-9421.