Délégation parlementaire
AU RENSEIGNEMENT

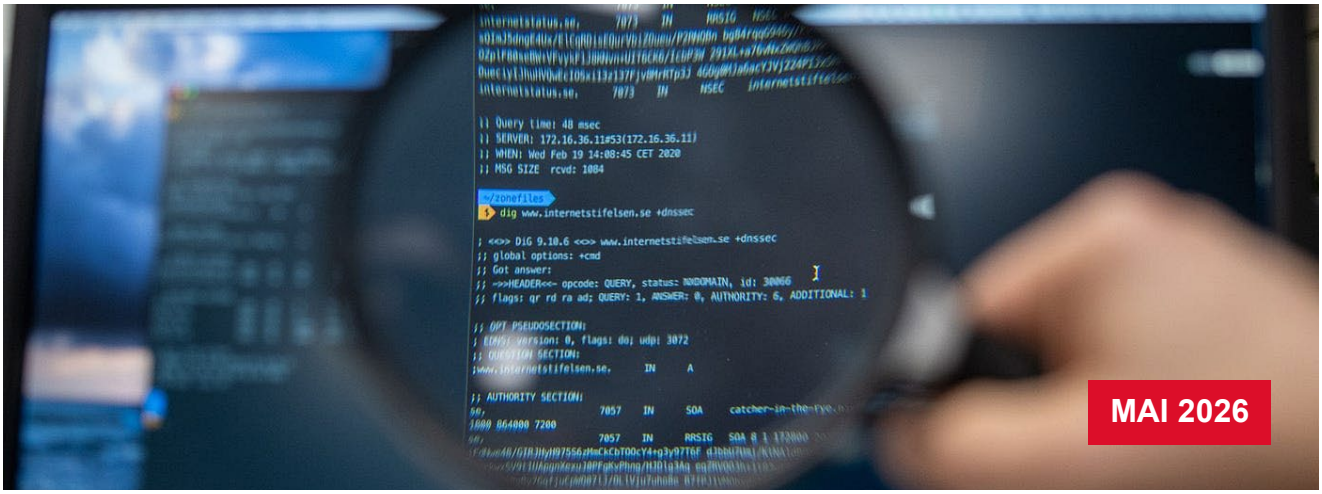
# Communication de la délégation parlementaire au renseignement

Sous la présidence de Muriel Jourda, sénateur, **la délégation parlementaire au renseignement a, depuis le début de l'année 2026, consacré ses travaux à l'évaluation du cadre juridique et de la mise en œuvre des techniques de renseignement, notamment la technique dite de l'**« **algorithme** », et à **la problématique du chiffrement** au regard de la politique publique du renseignement.

**Faisant usage des prérogatives qui lui sont reconnues par l'article 6 *nonies* de l'ordonnance du 17 novembre 1958**, la délégation a pu prendre connaissance des traitements algorithmiques mis en œuvre par les services de renseignement. Elle a également pu mesurer les conséquences opérationnelles du chiffrement sur les activités de renseignement et d'enquête.

Par la présente communication, **les membres de la délégation souhaitent verser au débat les éléments qui suivent afin d'éclairer le grand public et les travaux du Parlement sur ces enjeux**, en vue notamment de l'examen du projet de loi *actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense* et du projet de loi *relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.*

**Ces éléments feront l'objet de plus amples développements dans le rapport annuel de la délégation**, qui sera publié au début de l'année 2027.



# I. Messageries chiffrées : un accès ciblé des services de renseignement et de la justice est à la fois légitime et nécessaire

## A. Un accès ciblé au contenu des messageries chiffrées, un enjeu majeur pour la sécurité nationale

### 1. Le chiffrement, un défi pour les services de renseignement et l'autorité judiciaire

**Le chiffrement permet de garantir la confidentialité des échanges et des données**. Il est par conséquent un élément **déterminant de la sécurité informatique et la garantie de notre souveraineté**.

> **97 %**
>
> des messages envoyés par des téléphones portables le sont au moyen d'applications de messagerie, dont entre 60 à 80 % sont chiffrées de bout en bout[1]

Au cours des dernières années, **le recours à des solutions chiffrées s'est généralisé et constitue aujourd'hui la norme** pour une grande partie des communications numériques. Il devrait encore s'étendre avec le protocole RCS[2], qui devrait progressivement remplacer les SMS.

La plupart de ces services reposent sur **des protocoles de chiffrement dits « de bout en bout »** : le message est chiffré sur le terminal de l'expéditeur et ne peut être déchiffré que sur celui du destinataire. Ni le fournisseur du service, ni l'opérateur de télécommunications n'a accès aux contenus échangés pendant leur transmission.

Or, ainsi que la délégation a pu le constater à l'occasion des travaux qu'elle a menés, **l'impossibilité d'accéder au contenu des communications chiffrées constitue un obstacle majeur pour l'activité de la justice et des services de renseignement**.

Ainsi que l'exposait la Commission nationale de contrôle des techniques de renseignement (CNCTR) dans son rapport d'activité pour 2023[3], « ***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*** ».

**Cette vulnérabilité est parfaitement intégrée par nos adversaires, dans tout le spectre des menaces pour les intérêts fondamentaux de la Nation**[4]. Au-delà de la criminalité organisée, **le recours aux solutions de messagerie chiffrées « grand public » s'observe dans tous les domaines** : extrémisme violent, terrorisme, espionnage, ingérences étrangères, prolifération des armes conventionnelles ou de destruction massive, atteintes aux intérêts économiques de la France, etc.

---

[1] Rapport final du groupe d'experts de haut niveau sur l'accès aux données en vue d'une répression efficace créé par le Conseil de l'Union européenne, 15 novembre 2024.
[2] *Rich communication services.*
[3] Commission nationale de contrôle des techniques de renseignement, *8e rapport d'activité – 2023*, juin 2024, p. 146.
[4] La CNCTR (*id.*) rappelait à cet égard que ces outils numériques « *permettent à nos ennemis de mettre en réseau leurs actions, de mieux les dissimuler et de contourner les surveillances* ».

**Un cadre juridique obsolète**

L'article L. 871-1 du code de sécurité intérieure (CSI) impose aux *« personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité* », de remettre aux services de renseignement dûment autorisés, « *les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies* »*.*

Ces dispositions sont inappliquées car largement obsolètes. D'une part, la terminologie employée – « conventions de déchiffrement » – ne correspond pas à la réalité du fonctionnement des services utilisant le chiffrement de bout en bout. D'autre part, l'article L. 871-1 permet aux opérateurs de s'exonérer du respect de cette obligation s'ils « *démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions* » ; les fournisseurs de services chiffrés de bout en bout peuvent ainsi soutenir que ce procédé y fait obstacle.

### 2. L'absence d'alternative permettant actuellement de répondre aux besoins des services

À défaut du contenu des échanges, les services d'enquête et de renseignement peuvent avoir accès aux « métadonnées » (ou données de connexion), qui portent sur les circonstances de la communication[1], dont l'obtention est néanmoins tributaire de la coopération des plateformes (cf. *infra*). Si elles peuvent s'avérer particulièrement utiles dans le cadre d'une enquête ou du suivi d'une personne ou d'un réseau, **les métadonnées ne sauraient constituer un substitut au contenu des communications**.

Par exemple, des enquêteurs et certains parquets ont souligné qu'ils étaient souvent privés d'éléments probatoires indispensables pour établir l'implication d'un commanditaire ou de complices éloignés géographiquement des faits. Les services de renseignement se heurtent à des difficultés comparables. Les contourner impose de recourir à des techniques plus complexes : celles-ci ne sont pas adaptées à certaines situations qui appellent une intervention urgente.

À ce titre, **la technique dite du « recueil des données informatiques »** (RDI), qui constitue le principal moyen d'action permettant d'accéder au contenu des communications chiffrées[2], **ne représente pas, en l'état, une alternative satisfaisante**.

Plus intrusive, cette technique est employée de manière subsidiaire, comme le prévoit l'article L. 853-2 du CSI. En outre, comme la délégation a pu le constater, elle est techniquement complexe, coûteuse et consommatrice en moyens humains[3] : en conséquence, **sa mise en œuvre à l'échelle nécessaire paraît inenvisageable dans les conditions actuelles**[4].

---

[1] Figurent parmi ces données, qui diffèrent selon les services : l'identifiant du compte et les coordonnées de rattachement, l'adresse IP de connexion, la date des échanges, les informations relatives au terminal, etc.

[2] Cette technique recouvre en réalité des modes opératoires distincts, parmi lesquels figure le « piégeage » d'un terminal, qui est susceptible de permettre l'accès à la totalité de l'activité et du contenu de l'appareil.

[3] Ce constat a été renouvelé par la commission de vérification des fonds spéciaux (CVFS) dans son rapport annuel pour 2025, dont la plus grande partie des dispositions est classifiée.

[4] Les 5 715 avis rendus en 2024 par la CNCTR (contre 2 418 en 2020, soit une augmentation de 136 %) sur des demandes ayant pour objet le recours à la technique du RDI – qui ne préjugent pas de la mise en œuvre effective de la technique – doivent être mis en perspective avec les 14 316 avis rendus sur des interceptions de sécurité (les « écoutes téléphoniques »).

**Une coopération insuffisante de la part des opérateurs**

**La coopération avec les services de renseignement et la justice varie fortement selon les plateformes et dépend de leur politique interne**, qui est **totalement discrétionnaire**. Certaines s'arrogent le droit d'apprécier le bien-fondé ou la légalité des demandes dont elles sont saisies, quand d'autres refusent par principe toute transmission de données aux autorités.

À cet égard, la délégation s'étonne de ce qu'elle regarde comme **un double discours des principaux acteurs du secteur**.

D'une part, il est constant que **certaines plateformes, y compris lorsqu'elles font droit aux demandes des autorités, ne communiquent pas l'intégralité des données auxquelles elles ont pourtant accès**. Tel est notamment le cas des données de contenu qui ne sont pas chiffrées – à l'instar de systèmes de sauvegarde ou de messageries dans lesquels le chiffrement de bout en bout est optionnel ou inexistant – ou de certaines métadonnées.

D'autre part, **certaines plateformes coopèrent avec des autorités étrangères, tout particulièrement les autorités américaines** qui, en vertu du *Cloud Act* de 2018, ont accès aux données présentes sur leurs serveurs, et notamment un grand nombre de métadonnées.

Aux yeux des membres de la délégation, **il est essentiel de réduire l'écart qui s'est creusé entre les capacités d'investigation et de surveillance** des services de renseignement et de l'autorité judiciaire **et les outils à la disposition de nos adversaires**, dans un contexte de renforcement des menaces pesant sur la sécurité et l'indépendance nationales.

## B. L'objectif d'un accès ciblé et encadré, dont les conditions doivent être explorées à l'échelle européenne et dans le cadre d'un dialogue exigeant avec les plateformes

La délégation est d'avis qu'**un dispositif permettant un accès ciblé à certains contenus chiffrés** et qui ne se traduirait pas par un abaissement généralisé du niveau de sécurité **serait à même de garantir un juste équilibre entre**, d'une part, **la protection des libertés publiques et**, d'autre part, **la défense des intérêts fondamentaux de la Nation et la recherche des auteurs d'infractions graves**[1].

Elle souligne qu'**un tel accès ciblé ne serait pas différent, dans son principe, des interceptions sur les réseaux téléphoniques**, pour lesquelles la loi admet de longue date la possibilité de porter atteinte au secret des correspondances. Sa mise en œuvre serait soumise aux mêmes garanties que les interceptions de sécurité (soit les « écoutes téléphoniques »), notamment l'autorisation par le Premier ministre après avis de la CNCTR.

[1] Un tel dispositif respecterait les exigences tirées de la décision *Podchasov* de la Cour européenne des droits de l'homme (CEDH, 13 février 2024, n° 33696/19).

**Un encadrement strict du recours aux techniques de renseignement**

Les techniques de renseignement ne peuvent être mises en œuvre que par **les services habilités** et pour **l'une des sept finalités définies par l'article L. 811-3 du CSI**, qui participent de la **défense et de la promotion des intérêts fondamentaux de la Nation**.

Leur mise en œuvre fait l'objet d'une **autorisation délivrée par le Premier ministre après avis d'une commission indépendante, la CNCTR**. Centralisées par le groupement interministériel de contrôle (GIC), **les demandes sont motivées** : elles précisent notamment la nature de la technique, la finalité poursuivie, ses motifs ainsi que l'identité de la personne visée – éléments qui sont contrôlés par la CNCTR. Si le Premier ministre choisit de passer outre un avis défavorable, la décision d'autorisation ne peut être exécutée qu'après qu'une formation spécialisée du Conseil d'État, saisie par la CNCTR, a statué sur la demande.

À l'issue de ses travaux, **la délégation estime qu'un tel accès ciblé ne paraît pas inenvisageable sur le plan technique**[1]. **Des travaux sont en cours au niveau européen**, au sein d'un groupe d'experts constitué par la Commission européenne **aux fins d'élaborer une feuille de route technologique destinée à identifier des solutions permettant un tel accès**.

La délégation estime que **l'échelle européenne paraît la plus adaptée** pour obtenir **l'intégration d'outils permettant un accès ciblé à certains contenus chiffrés**. Elle invite par conséquent le Gouvernement à **poursuivre les démarches engagées avec les partenaires européens** en ce sens.

Il demeure toutefois nécessaire **de mener, au niveau national, un dialogue exigeant avec les plateformes** en vue d'un renforcement dans leur coopération avec les services de renseignement et l'autorité judiciaire, **sans exclure une initiative législative** en cas de blocage persistant.

### C. L'article 16 *bis* du projet de loi « résilience » : un risque majeur pour la politique publique du renseignement

Issu d'un amendement adopté en séance publique par le Sénat, l'article 16 *bis* du projet de loi *relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité*, dans sa rédaction issue des travaux de la commission spéciale de l'Assemblée nationale, prévoit qu'il « *ne peut être imposé aux fournisseurs de services de chiffrement, y compris aux prestataires de services de confiance qualifiés, l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques tels que des clés de déchiffrement maîtresses* ***ou tout autre mécanisme ou processus permettant un accès non consenti aux données protégées*** ».

La délégation observe que **le dispositif de cet article paraît aller au-delà des ambitions initiales de ses auteurs**, à savoir interdire toute obligation nouvelle d'introduire des « portes dérobées » dans les messageries chiffrées – obligation qui, en l'état du droit, n'existe pas.

[1] Compte tenu de la diversité des systèmes de messagerie, il serait envisagé, plutôt que d'imposer une solution technique unique, de laisser les plateformes retenir une solution parmi un ensemble d'options proposées et certifiées par les autorités.

**Or les techniques de renseignement**, qu'il s'agisse des interceptions téléphoniques, du RDI, de la géolocalisation ou du recueil des données de connexion, **ont précisément pour objet un accès** « ***non consenti*** » **à des** « ***données protégées*** » – cette dernière notion allant au-delà des seules données chiffrées. L'article L. 871-6 du CSI fait par ailleurs obligation aux opérateurs de télécommunications d'apporter leur concours à la mise en œuvre de ces techniques de renseignement.

S'il ne revient pas directement sur les dispositions législatives qui les régissent, **l'article 16 *bis* fragiliserait le cadre juridique des techniques de renseignement et d'enquête et entraverait leur mise en œuvre**. En outre, **son adoption enverrait un signal négatif aux opérateurs et aux plateformes et risquerait de se traduire par une moindre coopération**, y compris dans le cadre juridique actuel.

**Pour ces raisons, les membres de la délégation estiment que la rédaction actuelle de l'article 16 *bis* du projet de loi *relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité* présente un risque majeur pour la politique publique du renseignement.**

## II. L'algorithme : une technique strictement encadrée

Prévue à l'article L. 851-3 du CSI, la technique de l'algorithme a été introduite par la loi du 24 juillet 2015 *relative au renseignement*, avant d'être pérennisée en 2021. Cette technique a pour objet, comme le rappelait Jean-Jacques Urvoas, de « *recueillir, traiter, analyser et recouper un grand nombre d'éléments techniques anonymes pour détecter des signaux de faible intensité sur les données brutes qui témoigneraient d'une menace pesant sur la sécurité nationale* »[1].

Si la notion d'algorithme a pu nourrir certaines représentations fantasmées, de la « boîte noire » à la surveillance de masse, **la délégation a pu constater, à la lumière de ses travaux, une réalité plus circonscrite**.

### A. Un outil d'aide à la décision humaine, loin des fantasmes d'une surveillance généralisée

#### 1. Derrière le mythe de la boîte noire, un traitement dont chaque rouage demeure saisi par l'intervention humaine

Comme le relevait Philippe Bas dans son rapport sur le projet de loi de 2015, « *un algorithme est d'abord un programme, c'est-à-dire qu'à partir de paramètres préalablement établis, il donne un résultat attendu* »[2]. Le traitement algorithmique constitue ainsi **un simple outil de croisement de données**, qui applique une suite finie d'instructions elles-mêmes fondées sur l'expérience opérationnelle des services.

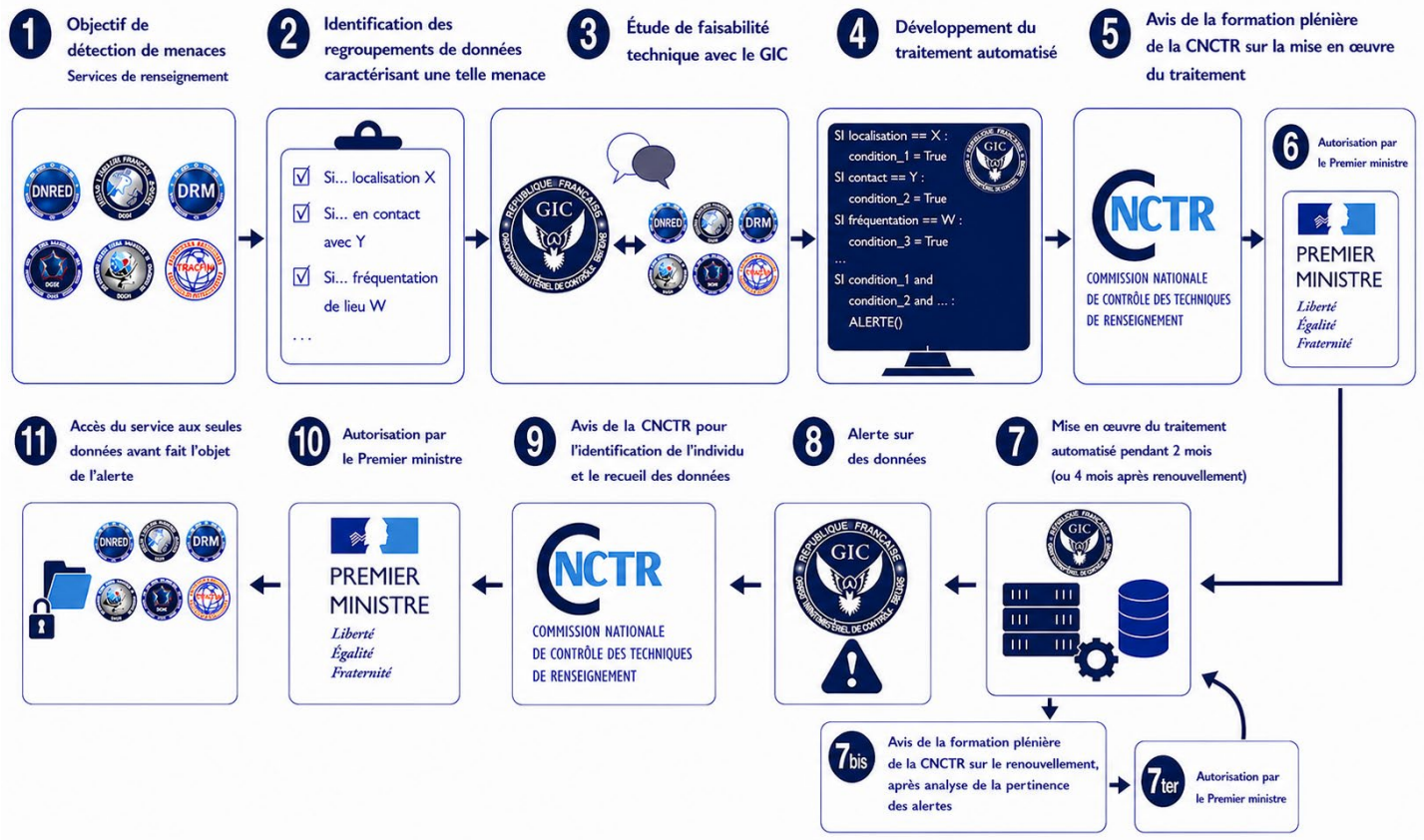
La délégation, qui a pu prendre connaissance des paramètres retenus pour certains traitements mis en œuvre, constate que ces dispositifs, **loin de constituer une « boîte**

---

[1] Rapport n° 2697 (XIVe législature) de M. Jean-Jacques Urvoas, fait au nom de la commission des lois de l'Assemblée nationale, avril 2015, p. 42.
[2] Rapport n° 460 (2014-2015) de M. Philippe Bas, fait au nom de la commission des lois du Sénat, mai 2015, page 88.

**noire » échappant à toute maîtrise humaine, reposent au contraire sur des critères et des cas d'usage strictement ciblés.** La détermination de ces paramètres résulte alors d'un **processus approfondi de conception et de validation retracé ci-après.**

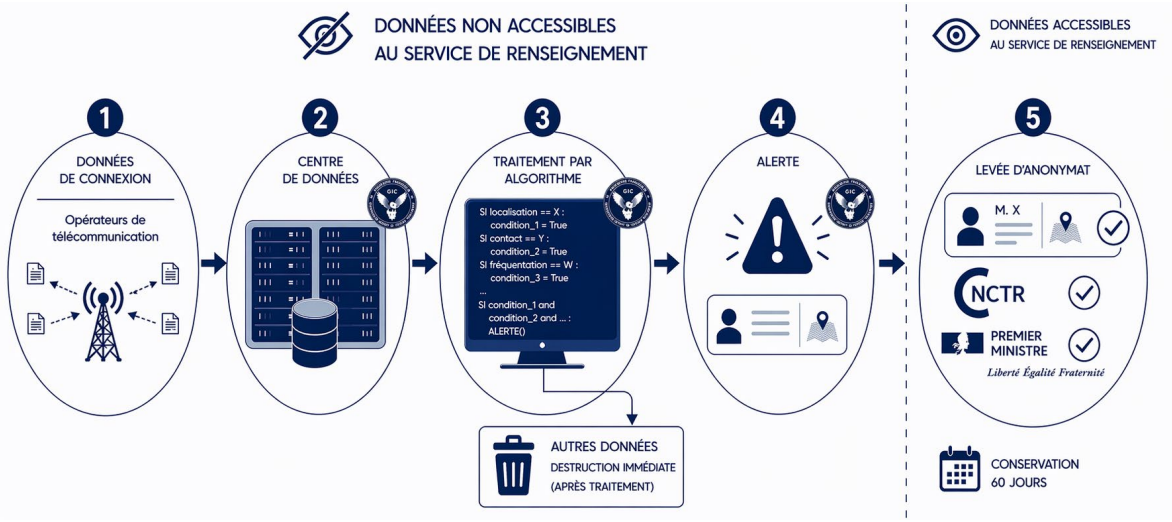
La délégation relève notamment que le **dialogue étroit qui s'établit, dès la conception de l'algorithme, entre la CNCTR, le groupement interministériel de contrôle (GIC) et le service concerné**, permet d'en sécuriser le paramétrage. Après son déploiement, la CNCTR dispose également d'un accès permanent au traitement et aux informations recueillies, conformément à l'article L. 851-3, lui permettant d'exercer un contrôle continu.




### 2. Un accès aux données strictement limité, excluant toute logique de surveillance généralisée

Il importe de rappeler que **les données traitées par les algorithmes**, lesquelles ne sont au demeurant que **des données de connexion (ou métadonnées)**, **demeurent inaccessibles aux services de renseignement**, tant en droit qu'en pratique dès lors qu'elles sont centralisées par le GIC. Seules les données à l'origine d'une alerte peuvent, le cas échéant, leur être transmises, toutes les autres sont immédiatement détruites.

À cette première garantie s'ajoute l'exigence d'une **autorisation préalable pour accéder aux informations issues de l'alerte**, dont les échanges conduits avec la CNCTR ont confirmé l'intérêt, en ce qu'elle permet de veiller en temps réel au volume de signalements générés.




La technique de l'algorithme **ne saurait ainsi être assimilée à une surveillance de masse, dans la mesure où elle ne vise ni la constitution d'une base pérenne d'informations sur l'ensemble de la population, ni la connaissance des activités d'une multitude de personnes identifiables**.

## B. Un outil en construction, dont la délégation estime qu'il n'a pas encore donné toute sa mesure

### 1. Une technique dont les usages se précisent

La technique de l'algorithme présente **un intérêt réel au regard de l'évolution des menaces**, désormais plus diffuses, à l'image de la menace terroriste. Elle se distingue en effet des autres techniques en ce qu'**elle permet non pas de surveiller des cibles, mais de détecter des comportements échappant alors aux moyens de surveillance traditionnels**.

Le nombre de traitements autorisés demeure pour autant relativement limité. La délégation a pris connaissance de **la mise en service de huit algorithmes depuis 2017, dont six sont encore en fonctionnement**.

Cette progression mesurée s'explique en grande partie par **le temps nécessaire à la conception, estimé à environ dix-huit mois**, ainsi que l'importante mobilisation de ressources humaines**. Cette situation ne se traduit toutefois pas par un désintérêt des services pour cette technique**. Plusieurs ont indiqué à la délégation avoir entamé une réflexion en ce sens. La mise en service de **deux nouveaux traitements en 2025**, et la perspective de nouveaux déploiements en 2026, confirment cette dynamique.

Le retour d'expérience apparaît toutefois **encore inégal selon les finalités poursuivies**, tous les algorithmes n'ayant pas donné, à ce stade, les résultats escomptés. La délégation estime néanmoins qu'**il serait prématuré d'en tirer des conclusions définitives**, compte tenu du temps requis pour le calibrage des traitements**.** À ce délai d'ajustement s'ajoute le fait que les évolutions récentes du cadre légal n'ont pas encore produit tous leurs effets : initialement limitée à la prévention du terrorisme, les finalités autorisées n'ont été élargies qu'en juillet 2024[1], tandis que le périmètre des données mobilisables a été modifié à plusieurs reprises.

[1] La loi du 25 juillet 2024 a étendu, à titre expérimental et jusqu'au 1er juillet 2028, l'emploi de cette technique aux finalités liées à la prévention des menaces pour la défense nationale et aux ingérences étrangères.

### 2. L'extension du champ des données traitées aux URL : une évolution attendue

Les adresses de ressources sur internet (URL[1]) constituent une donnée issue de la navigation en ligne. La délégation a pu constater que **l'exploitation de ces adresses,** qu'elles renvoient par exemple à la consultation de contenus de propagande terroriste ou qu'elles révèlent, par leur structure même, un mode opératoire utilisé dans le cadre de cyberattaques**, présentent un intérêt avéré pour la caractérisation de la menace**.

Cette réflexion n'est pas nouvelle. Dès 2020, les services de renseignement faisaient valoir que les résultats encore limités de la technique algorithmique tenaient en partie au champ trop restreint des données analysables[2]. C'est dans cet esprit que **la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement avait ouvert la possibilité de recourir aux URL.**

**Cette faculté a toutefois été remise en cause par la décision du Conseil constitutionnel du 12 juin 2025 portant sur la loi dite « *Narcotrafic* »**[3]. Ce dernier a notamment mis en avant le fait que ces dispositions permettaient une analyse à grande échelle de données susceptibles de révéler le contenu des correspondances, en raison du caractère « mixte » des URL[4]. Les URL regroupent en effet, au sein d'une même ligne, des éléments relatifs à l'acheminement de la communication, soit des données de connexion, et d'autres susceptibles de renseigner sur le contenu consulté.

Tirant les conséquences de cette décision, l'article 18 du projet de loi *actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense* prévoit de **circonscrire les URL susceptibles d'être mobilisées aux seules adresses dont l'exploitation présente**, selon une typologie précisément définie, **un lien avec la menace.**

La délégation partage l'analyse selon laquelle **la décision du Conseil constitutionnel n'exclut pas par principe tout recours aux URL mais invite plutôt le législateur à encadrer davantage les données susceptibles d'être utilisées**[5]. Elle relève également que **la dissociation des composantes d'une URL** afin de distinguer les données de connexion de celles liées au contenu consulté n'est pas réaliste, une telle solution étant **à la fois techniquement impraticable et de nature à priver largement le dispositif de son utilité.**

Elle observe ainsi que l'approche retenue par le projet de loi assure un **équilibre satisfaisant entre les exigences de protection de la vie privée et celles de prévention des menaces**.

**Pour ces raisons, les membres de la délégation approuvent l'utilisation des URL dans les traitements algorithmiques dans les conditions prévues à l'article 18 du projet de loi *actualisant la programmation militaire pour les années 2024 à 2030*.**

---

[1] *Uniform resource locator.*
[2] Rapport du Gouvernement au Parlement sur l'application de l'article L. 851-3 du CSI, transmis le 30 juin 2020.
[3] Conseil constitutionnel, n° 2025-885 DC du 12 juin 2025, cons. 127 à 129.
[4] La qualification de « données mixtes » concernant les URL a été retenue autant par la CNIL (Délibération n° 2015-455 du 17 décembre 2015) que la CNCTR (délibération n° 1/2016 du 14 janvier 2016).
[5] Le commentaire de cette décision n° 2025-885 précise, en ce sens, que le Conseil constitutionnel « *n'a pas entendu opposer une interdiction définitive du recours aux traitements algorithmiques, même pour traiter des « URL », mais l'a subordonné à un encadrement nettement plus précis des types de données susceptibles d'être recueillies, par le législateur lui-même (et non en reportant les garanties sur la seule effectivité du contrôle confié à la CNCTR).* » (page 18)

## POUR EN SAVOIR PLUS

La **délégation parlementaire au renseignement** comprend huit membres, quatre sénateurs et quatre députés. Elle a pour mission de contrôler l'action du Gouvernement en matière de renseignement, d'évaluer la politique publique en ce domaine et d'assurer un suivi des enjeux d'actualité et des défis à venir qui s'y rapportent.

Quatre de ses membres sont désignés pour siéger à la commission de vérification des fonds spéciaux (CVFS) afin de vérifier que les dépenses faites sur les fonds spéciaux sont conformes à la destination qui leur a été assignée par la loi de finances.

Les travaux de ces deux organes sont couverts par le secret de la défense nationale.

# Composition de la délégation parlementaire au renseignement

### *Les quatre membres de droit*

**Muriel JOURDA**
**Présidente**
Présidente de la commission des lois
Sénateur du Morbihan
Les Républicains

**Cédric PERRIN**
Président de la commission des affaires étrangères, de la défense, et des forces armées
Sénateur du Territoire de Belfort
Les Républicains

**Florent BOUDIÉ**
**1er Vice-Président**
Président de la commission des lois
Député
(10e circonscription de Gironde)
Ensemble pour la République

**Jean-Michel JACQUES**
Président de la commission de la défense et des forces armées
Député
(6e circonscription du Morbihan)
Ensemble pour la République

### *Les quatre membres désignés*

**Agnès CANAYER**
Sénateur de la Seine-Maritime
Les Républicains (Ratt.)

**Gisèle JOURDA**
**Vice-Présidente**
Sénatrice de l'Aude
Socialiste, Écologiste et Républicain

**Caroline COLOMBIER**
Députée
(3e circonscription de Charente)
Rassemblement national

**Aurélien ROUSSEAU**
Député
(7e circonscription des Yvelines)
Socialistes et apparentés (App.)