Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 118/2025 du 12 novembre 2025

Objet : Avis concernant un projet d'arrêté royal fixant les règles de destruction des données obtenues illégalement visées à l'article 44/4 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et fixant les règles de coopération visées à l'article 44/5 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (CO-A-2025-104).

Mots-clés : interception de communications électroniques ; coopération des opérateurs et fournisseurs de services de communications électroniques ; chiffrement ; réseaux ; sécurité nationale ; services de renseignements et de sécurité.

Version originale

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier ses articles 23 et 26 (ci-après « LCA ») ;

Vu le 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, et abrogeant la directive 95/46/CE* (ci-après « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis de Madame Vanessa Matz, Ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'Etat, du Numérique et de la Politique scientifique, reçue le 24 juillet 2025 ;

Vu la demande d'informations complémentaires adressée au demandeur le 2 septembre 2025 ;

Vu les réponses communiquées par le demandeur le 15 septembre 2025 ;

Vu la demande d'informations complémentaires adressée au demandeur le 15 septembre 2025 ;

L'Autorité ne publie en français et en néerlandais que les avis concernant les projets ou propositions de textes de rang de loi émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale ou de la Commission Communautaire Commune. La « Version originale » est la version qui a été validée.

Vu les réponses communiquées par le demandeur le 17 septembre 2025 ;

Vu la sollicitation de Monsieur Bart Preneel (ci-après « l'Expert désigné par l'Autorité ») en tant qu'expert le 25 septembre 2025, conformément à l'article 18/1 de la LCA et aux articles 3 et 4 du Règlement d'ordre intérieur de l'Autorité de protection des données ;

Vu la demande d'informations complémentaires adressée au demandeur le 5 octobre 2025 ;

Vu les réponses communiquées par le demandeur le 9 octobre 2025 ;

Vu la communication par l'Expert désigné par l'Autorité de son rapport le 3 novembre 2025 ;
Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 12 novembre 2025, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant un projet d'arrêté royal *fixant les règles de destruction des données obtenues illégalement visées à l'article 44/4 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et fixant les règles de coopération visées à l'article 44/5 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité* (ci-après, « **le Projet** »).

2. L'article 44/5 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après, « **la Loi R&S** ») concerne **le concours d'opérateurs de réseau ou fournisseurs de services de communications électroniques** dans le cadre de l'interception des communications émises ou reçues à l'étranger, visée à l'article 44 de la Loi R&S. Cette dernière disposition vise la possibilité pour le Service Général du Renseignement et de la Sécurité (ci-après, « **le SGRS** ») de « *rechercher, capter, écouter, prendre connaissance et enregistrer toute forme de communications* ***émises ou reçues à l'étranger****, selon les modalités fixées aux articles 44/3 et 44/4, dans le cadre des missions visées à l'article 11, § 1er, 1° à 3° et 5°* » (mis en gras par l'Autorité). Ces interceptions sont **principalement réalisées sur la base d'une liste annuelle d'organisations ou d'institutions**.

3. L'article 44/5, al. 1er, de la Loi R&S prévoit que « ***Si une opération sur un réseau de communications est nécessaire pour permettre l'interception*** *de communications émises ou reçues à l'étranger visée à l'article 44, l'opérateur du réseau ou le fournisseur du service de communications*

électroniques est saisi d'une demande écrite du dirigeant du service et est tenu de prêter son concours dans les plus brefs délais » (mis en gras par l'Autorité). Le Projet exécute le dernier alinéa de cet article selon lequel le Roi fixe, sur la proposition du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, les modalités du concours de l'opérateur ou du fournisseur concerné.

4. En synthèse, le Projet prévoit, afin d'organiser l'interception des communications électroniques (méta-données et contenu) souhaitées, **une sélection suivie d'un double filtrage de flux de données de communications électroniques[1].** Une **sélection** de flux de données serait tout d'abord réalisée via des équipements placés sur l'infrastructure de réseau de l'opérateur ou fournisseur concerné, et ces flux seraient ensuite dupliqués vers des équipements du SGRS installés « chez » cet opérateur ou fournisseur. Ensuite, un **premier filtrage** de ces flux de communications serait réalisé via ces derniers équipements. Un **second filtrage** des données transférées, plus précis, serait alors mis en œuvre dans les installations du SGRS lui-même.

5. Les dispositions précitées ont été insérées dans la Loi R&S par la loi du 30 mars 2017 *modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259bis du Code pénal* (ci-après, « **Loi de 2017** »)[2].

6. Les dispositions alors en projet de la Loi de 2017 ont été l'objet de l'Avis de la Commission de la Protection de la Vie Privée n° 20/2016 du 18 mai 2016 *concernant un avant-projet de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (CO-A-2016-016)* (ci-après, « **l'Avis de la CPVP de 2016** »), d'un Avis du Comité permanent R *sur le projet de loi modifiant la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) (2017)*[3] (ci-après, « **l'Avis de 2017 du Comité R** ») et d'un avis du Conseil d'Etat n° 59.509/4 du 27 juin 2016 *sur un avant-projet de loi 'modifiant la loi du 30 novembre 1998 organique des services de*

---

[1] Voir les considérants nos 55 et 61.

[2] L'exposé des motifs de cette loi, s'agissant de l'interception des communications électroniques, indique notamment que :

« *Eu égard au fait que de plus en plus de communications transitent via câbles, y compris les fibres optiques, le SGRS se doit de développer de nouveaux procédés d'interception permettant ce qu'on appelle communément le "cable tapping". En effet, le SGRS ne peut pas se permettre de ne pas pouvoir intercepter les nombreuses communications circulant sur les câbles et rater, par la même occasion, des échanges entre cellules terroristes ou entre factions rebelles.*

La manière la plus efficiente et la plus rapide de faire du cable taping est de solliciter la collaboration des opérateurs de réseau et des fournisseurs de services de télécommunications. La collaboration de certains opérateurs actifs en Belgique, qui offrent des services de transmission par câble vers et de l'étranger, permettrait en effet plus facilement d'intercepter des flux de communications et de données émises à l'étranger. Ces flux seront filtrés par le SGRS sur la base du plan d'écoute afin de n'extraire que les communications et données émises à l'étranger et autorisées par ce plan et en lien avec les missions du SGRS.

Il s'agira donc toujours bien d'interceptions ciblées. Aucune captation de masse n'est légalement autorisée », *Doc. Parl.*, Ch. des Représentants, n° 54-2043/001, p. 89.

[3] Cet avis est disponible sur https://www.comiteri.be/index.php/fr/publications/avis, dernièrement consulté le 29/08/2025. Pour la rédaction de son avis, la CPVP avait obtenu communication de l'avis du Comité R qui n'était pas public (« *Beperkte verspreiding (K.B. 24 maart 2000)* »).

renseignement et de sécurité' (ci-après, « **l'Avis du Conseil d'Etat de 2016** »). Au stade de la rédaction du présent avis, le Comité R a rendu à propos du Projet un **Avis n° 002/CPR/2025 du 11 septembre 2025** (ci-après, « **l'Avis du Comité R** »)[4].

7. En l'occurrence, l'Autorité est bien **compétente s'agissant des traitements de données qui relèvent de la responsabilité des opérateurs de réseaux de télécommunications et des fournisseurs de services de communications électroniques**, nonobstant le fait que ceux-ci soient directement en relation avec les activités de traitement de données à caractère personnel du SGRS, soit relevant du Titre 3 de la LTD[5].

II. EXAMEN DU PROJET

Le présent avis est structuré comme suit :

[4] Cet avis est disponible sur https://www.comiteri.be/index.php/fr/publications/avis, dernièrement consulté le 20/10/2025. Le demandeur a indiqué que l'avis du Conseil d'Etat serait demandé en fin de processus, une fois le Projet consolidé sur la base des avis de l'Autorité et du Comité R ainsi que de l'avis reçu dans le cadre de la consultation publique.

[5] Voir par exemple, l'Avis n° 184/2021 du 4 octobre 2021 *concernant un avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (CO-A-2021-174)*, concernant les institutions qui ne sont pas des services de renseignement et de sécurité, et l'Avis n° 34/2024 du 15 avril 2024 *concernant une Proposition de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour (CO-A-2024-139)*. S'agissant des différents cadres normatifs en matière de protection des données, voir Autorité de Protection des Données, Service d'Autorisation et d'Avis, « », disponible sur https://www.autoriteprotectiondonnees.be/index.php/publications/brochure-informative-le-secteur-public-et-obligations-legales.pdf, dernièrement consulté le 01/09/2025, pp. 9-11, pp. 9-11.

Voir le **considérant n° 41**.

II.1. L'Avis de la CPVP de 2016

8. **En 2016, aux considérants nos 25 à 37 de son avis, la Commission de la Protection de la Vie Privée**, prédécesseuse de l'Autorité, **avait critiqué l'avant-projet de loi qui a donné lieu à la Loi de 2017**, s'agissant de l'interception des communications électroniques émises ou reçues à l'étranger, et de la collaboration des fournisseurs de services concernés en la matière.

9. A titre préliminaire, l'Autorité reprend ci-après l'essentiel des considérations pertinentes en la matière :

> « *B.5. Extension des prérogatives du SGRS à l'étranger*
>
> *B.5.1. Nouvelles méthodes ad hoc*
> *(articles 79 et 80 de l'avant-projet modifiant les articles 44bis et ter de la LRS)*
>
> *25. En marge des méthodes spécifiques et exceptionnelles de recueil de données, le SGRS est en outre compétent pour une méthode ad hoc lui permettant d'intercepter des communications émises à l'étranger, et ce, sous certaines conditions et moyennant un contrôle ad hoc (articles 259bis, § 5 du Code pénal, 44bis et ter de la LRS). Les interceptions s'effectuent selon un plan d'écoute annuel approuvé par le Ministre de la Défense et transmis au Comité R énumérant la liste des organisations et institutions qui feront l'objet d'interceptions.*
>
> *26.* […]
>
> *27. Il souhaite **introduire cette plus grande flexibilité** pour ces deux méthodes de collecte d'informations **au motif que** le SGRS n'est pas en mesure de suivre la procédure fixée pour recourir aux méthodes spécifiques et exceptionnelles pour différentes raisons: à l'étranger, décalage horaire, urgence, aucun moyen de communication sécurisé, impossibilité de cibler une personne ou un événement précis, …*
>
> *28. Le demandeur prévoit cependant de renforcer le contrôle ad hoc par une motivation plus développée de la liste annuelle et par l'envoi mensuel au Comité R d'une liste motivée contenant les pays ou organisations et institutions ayant fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images. Ainsi, le Comité R serait tenu de manière régulière au courant des écoutes, intrusions et prises d'images effectuées.*
>
> *29. La Commission rappelle qu'en principe l'intrusion dans un système informatique et la prise d'images sont soumis au contrôle administratif de la Commission BIM et au contrôle*

juridictionnel du Comité R. L'avant-projet va soustraire ces méthodes à ce contrôle pour le soumettre à un ***contrôle ad hoc moins étendu****.*

30. Elle remarque également que ces mesures ne sont pas ciblées ou du moins que l'intention n'est pas de les cibler sur des personnes identifiées mais sur des organisations et groupes. Il doit toutefois être clair que les trois méthodes de renseignement visées capteront inévitablement des données à caractère personnel.

31. Partant, elle émet des ***réserves quant à l'extension envisagée d'une procédure ad hoc qui par nature devrait rester circonscrite****.*

B.5.2. Extension de la possibilité d'intercepter des communications à l'étranger aux communications reçues à l'étranger
(article 76 de l'avant-projet (ré)introduisant l'article 44 de la LRS)

32. Dans le cadre de la méthode particulière évoquée précédemment d'interception par le SGRS de toute forme de communications émises à l'étranger, l'avant-projet prévoit ***d'étendre cette méthode aux communications reçues à l'étranger****.*

33. Suivant l'exposé des motifs, cette adaptation fait suite aux évolutions technologiques qui rendent pour les communications basées notamment sur le protocole IP difficilement exploitable le critère de base que représentait traditionnellement l'origine de la communication.

34. La Commission prend acte de cette explication mais constate que les prérogatives accordées au SGRS, et partant ***les possibilités d'intrusion dans la vie privée des personnes concernées, sont ce faisant fortement étendues, puisque des communications se déroulant exclusivement à l'étranger pourront également être interceptées****.*

B.5.3. Instauration d'une collaboration des opérateurs à l'étranger
(article 81 de l'avant-projet créant un nouvel article 44/5 de la LRS)

35. Alors que la collaboration des opérateurs est prévue pour la mise en œuvre des méthodes spécifiques et exceptionnelles, celle-ci n'est pas prévue pour la méthode particulière d'interception des communications émises (ou reçues) à l'étranger. ***L'insertion de ce nouvel article 44/5 vise à prévoir cette obligation de collaboration*** *dans le chef des opérateurs de réseau et des fournisseurs d'un service de communications électroniques qui offrent (également) un service de communications électroniques sur le territoire belge.*

36. ***L'intention du demandeur est de permettre au SGRS de procéder à ce qu'on appelle le « cable tapping »****, permettant d'intercepter l'ensemble des communications circulant sur les câbles.*

37. La Commission est ***défavorable à cette manière de procéder qui permettrait au SGRS d'intercepter un flux de données sans proportion avec la finalité poursuivie et qui commence fortement à s'apparenter à de la surveillance de masse. Il importe peu à cet égard que ces flux soient filtrés par le SGRS sur la base du plan d'écoute afin de n'extraire que les communications et données émises à l'étranger qui sont autorisées par ce plan et en lien avec les missions du SGRS. Contrairement à ce qui est mentionné dans l'exposé des motifs, le texte de loi permet en soi bel et bien qu'il soit procédé à de la captation de masse*** » (mis en gras par l'Autorité).

II.2. L'hypothèse concernée

II.2.1. Missions du SGRS concernées

10. Comme le Conseil d'Etat l'a souligné à deux reprises, **les missions de renseignement sont définies de manière fort large par les articles 7, 8 et 11 de la L.R&S, de sorte qu'elles doivent être interprétées de manière prudente** et dans le strict respect des principes de subsidiarité et de proportionnalité lorsqu'il s'agit de recourir aux méthodes spécifiques et exceptionnelles de recueil de données[6]. En l'occurrence, l'interception[7] de communications électroniques à l'étranger par le SGRS peut avoir lieu dans le cadre des **missions visées à l'article 11, § 1er, 1° à 3° et 5° de la L.R&S**. Il est à noter que la Loi de 2017, en même temps qu'elle a consacré des dispositions particulières à l'exercice des missions du SGRS, a également étendu la compétence de celui-ci.

11. Les missions concernées en droit positif par l'interception des communications électroniques sont les suivantes :

> « *1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer:*
> *a) l'intégrité du territoire national ou la population,*

[6] Voir l'Avis du Conseil d'Etat de 2016, et l'Avis du Conseil d'Etat n° 42.178/2 du 19 février 2007 *sur un avant-projet de loi 'relatif aux méthodes de recueil des données des services de renseignement et de sécurité'.*

[7] La compétence du SGRS ne se limite pas à l'interception, voir le considérant n° 2.

b) les plans de défense militaires,
c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,
d) l'accomplissement des missions des Forces armées,
e) la sécurité des ressortissants belges à l'étranger,
f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité ;
et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense ;

2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés ;

2° /1 de neutraliser, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par le ministre de la Défense et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international ;

3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère ;

[...]

5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge »[8].

12. Dans la lignée de la position exprimée par le Conseil d'Etat et compte-tenu de l'ingérence causée par les articles 44 et 44/5 de la Loi R&S (et à plus forte raison encore, le dispositif en projet, sans préjudice des commentaires ultérieurs quant au fondement légal et aux garanties encadrant ce dernier), l'Autorité est d'avis que **dans la mise en œuvre** de ces dispositions et **de la coopération des opérateurs et fournisseurs de services de communications électroniques, les missions du SGRS doivent être interprétées de manière prudente et dans le strict respect des principes de subsidiarité et de proportionnalité**.

II.2.2. Prestataires de services concernés par l'obligation de coopération

13. L'Autorité relève avant tout que comme l'exposé des motifs de la Loi de 2017 l'indique, **les types de services de communications électroniques** visés sont variés et nombreux, de sorte que les prestataires susceptibles de devoir coopérer avec le SGRS sont tout aussi variés et nombreux. En outre, sur le plan de la compétence territoriale, les prestataires de services sont soumis au dispositif concerné **dès qu'ils offrent leurs services en Belgique**. Plus en détails, l'exposé des motifs précité indique ce qui suit :

> « *Dans le projet est insérée une définition de "fournisseur de service de communications électroniques" (nouveau 11°/1) afin de délimiter le champ d'application personnel et territorial de l'obligation de collaboration du secteur télécom:*
>
> - *non seulement les fournisseurs classiques d'un service de communications électroniques, visés à l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques, tombent sous l'obligation de collaboration (**Proximus, Mobistar, Base, Telenet, Scarlet, VOO, Mobile Viking, les fournisseurs d'hotspots Wifi gratuits**…)*
> - *mais c'est également le cas de **tous les fournisseurs de services de communication alternatifs comme Yahoo, Hotmail, Gmail, Skype, Whats App, Viber, les jeux avec possibilité de chat…***
>
> *Est dès lors considéré comme fournisseur **quiconque fournit un service consistant à offrir à ses clients une possibilité d'échange électronique d'informations**.*

[8] L'article 11, § 2, de la Loi R&S définit certains concepts utilisés par cette disposition.

Concernant le champ d'application territorial, il convient de souligner que l'obligation de collaboration est d'application à quiconque propose un service de communication en Belgique. La présence du fournisseur sur le territoire belge n'est par conséquent pas requise.

La définition insérée dans la loi est reprise de l'arrêt de la Cour d'appel d'Anvers du 20 novembre 2013 dans lequel elle estime que Yahoo est le fournisseur d'un service de communications électroniques au sens de l'article 46bis du Code d'instruction criminelle (l'équivalent de l'article 18/7 de la loi relative aux services de renseignement et de sécurité) et est soumis à la législation belge parce qu'il met ses services à disposition en Belgique. Cet arrêt a été confirmé par la Cour de cassation le 1er décembre 2015 »[9].

14. Outre les fournisseurs de services de communications électroniques, sont ainsi plus « classiquement » et également visés **les opérateurs de réseau**, soit les entités qui fournissent un réseau de communications électroniques tel que défini à l'article 2, 3°, de la Loi du 13 juin 2005 relative aux communications électroniques[10]. De la même manière, pour entrer dans le champ d'application territorial de la collaboration concernée, il suffit que ces opérateurs offrent leurs services en Belgique.

15. A la demande de l'Autorité, le demandeur **a confirmé que n'étaient permises que les interceptions de communications électroniques transitant <u>via ces services accessibles en Belgique</u>**, et non via d'autres services éventuellement fournis par le fournisseur ou l'opérateur concerné. Ceci **doit être clarifié dans le dispositif** du Projet. Autrement dit par exemple, si un fournisseur de services offre un service de type A (accès à internet) à l'étranger mais un autre service de type B (courriel) en Belgique, il ne pourrait pas être contraint à collaborer avec le SGRS s'agissant de son service de type A. La collaboration d'un opérateur ou d'un fournisseur de service de communications électronique **<u>ne</u> pourra donc <u>pas</u> être sollicitée pour un service** (de communications électroniques ou un réseau) **exclusivement offert en dehors de la Belgique**, **et ce, <u>malgré</u>** le fait que le prestataire concerné offre d'autres services (de communications électroniques ou un réseau) en Belgique.

16. Dans le contexte juste exposé, la **localisation des installations des prestataires de services concernés** revêt une certaine importance dès lors que le Projet prévoit que le **<u>SGRS va installer lui-même</u> des équipements <u>« *chez* » ces prestataires</u>, et visiter ces derniers**. Dans ce cadre,

---

[9] *Doc. Parl.*, Ch. des Représentants, n° 54-2043/001, pp. 26-27.

[10] Soit « *les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de services de médias audiovisuels ou sonores* ».

si la mise en œuvre de la collaboration semble praticable lorsque l'opérateur ou le fournisseur concerné dispose d'installations en Belgique, l'Autorité a interrogé le demandeur quant à la question de savoir comment en pratique, il est envisagé d'assurer l'accès du SGRS à des installations d'opérateurs et fournisseurs situés à l'étranger, y compris l'installation chez ceux-ci, d'équipements ? Le demandeur a répondu que « ***Si l'opérateur/fournisseur n'a pas d'infrastructures (télécoms ou bureaux) en Belgique, il n'y aura pas de collaboration***. *Dans le cas contraire, il sera procédé à la coopération détaillée dans le projet d'arrêté royal* » (mis en gras par l'Autorité). Dans les réponses communiquées à la suite de la troisième demande d'informations complémentaires adressées par l'Autorité, le demandeur a précisé que « *Le concours des fournisseurs/opérateurs nécessite que les services soient disponibles sur le territoire national* ***et qu'il y ait dès lors une infrastructure en Belgique (même si celle-ci est louée ou partagée par le fournisseur ou l'opérateur)***. *Les communications faisant l'objet de la coopération entre le fournisseur ou opérateur et le SGRS seraient dans ce cas rapatriées jusqu'aux installation situées en Belgique* » (mis en gras et souligné par l'Autorité).

17. L'Autorité est par conséquent d'avis que le **dispositif du Projet doit être adapté et ne viser que la collaboration avec les opérateurs et fournisseurs de services de communications électroniques qui offrent leur service en Belgique et recourent à cette fin à une infrastructure technique pertinente au regard du service ou réseau concerné, sur le territoire belge et sur laquelle ils exercent un contrôle suffisant compte-tenu de la coopération envisagée**. En effet, dans son rapport, l'Expert désigné par l'Autorité indique également et notamment ce qui suit « *Aangezien er apparatuur van ADIV bij de operator moet geplaatst worden, is de duplicatie enkel mogelijk als de aanbieder van elektronische communicatiediensten of de operator over een fysieke infrastructuur op het Belgisch grondgebied beschikt* ***waarover hij voldoende controle heeft*** » (mis en gras par l'Autorité). Pour le reste, quant aux types de services concernés, elle prend acte du fait que la coopération prévue a pour objectif de **s'appliquer largement à quiconque fournit un service consistant à offrir à ses clients une possibilité d'échange électronique d'informations**.

II.2.3. « Décryptage » des communications – chiffrement

18. L'exposé des motifs de la Loi de 2017 indique que « *La collaboration vise notamment à permettre au SGRS d'installer ses équipements au sein de l'établissement de l'opérateur et de rendre l'interception possible, notamment via mise à disposition de bandes passantes et routage de flux* ***mais vise également à assister le SGRS dans le décryptage des communications*** »[11] (mis en gras par l'Autorité). **Cependant, l'article 44/5 de la L.R&S ne vise qu'à** « ***permettre l'interception*** » des communications électroniques.

[11] P. 90.

19. L'Autorité a invité le demandeur à confirmer que le Projet **ne** vise **pas** la coopération des opérateurs et fournisseurs afin de **déchiffrer des communications électroniques**. Celui-ci a répondu ce qui suit à la première demande d'informations complémentaires adressée par l'Autorité :

> « ***La coopération décrite à l'article 44/5*** *de la loi du 30 novembre 1998 vise l'opération sur le réseau de communications du fournisseur/opérateur permettant au SGRS de* ***rechercher, capter, écouter, prendre connaissance et enregistrer*** *toute forme de communications émises ou reçues à l'étranger. Cette disposition vise donc les actes techniques permettant au SGRS de capter, écouter et enregistrer les communications transitant par les réseaux de l'opérateur ou du fournisseur, en ce compris l'installation d'équipements, la mise à disposition de bande passante ou le routage des flux. En revanche, elle* ***n'impose pas une obligation générale d'assistance au décryptage, notamment lorsque les communications sont chiffrées de bout en bout par des moyens externes au fournisseur****. Une assistance limitée peut toutefois être envisagée lorsque le fournisseur lui-même applique le chiffrement et détient les moyens de le lever, ce qui s'inscrit encore dans la logique de « permettre l'interception » au sens technique****. En conclusion, le projet* ***ne prévoit pas d'obligation générale pour les opérateurs ou fournisseurs de coopérer au déchiffrement de communications électroniques, sauf si cela découle directement de leurs propres mécanismes de chiffrement*** » (mis en gras et souligné par l'Autorité).

20. Cette réponse appelle les cinq commentaires suivants. **Premièrement**, l'Autorité souligne que les articles 44 et 44/5 de la Loi R&S, insérés par une même loi, sollicitent clairement des concepts distincts. Tandis que l'article 44 attribue une large compétence au SGRS pour « *rechercher, capter, écouter, prendre connaissance et enregistrer* » certaines communications, l'article 44/5 de la Loi R&S ne vise le concours de l'opérateur ou du fournisseur de service que « *si une opération* ***sur un réseau*** *de communications est nécessaire pour permettre* ***l'interception*** *de* [ces] *communications* » (mis en gras par l'Autorité). **Autrement dit, l'Autorité est d'avis que l'interprétation proposée par le demandeur pose question** : **le concours de l'opérateur étant limité à l'interception de communications**. Remarque : dans le sens de l'interprétation suivie par l'Autorité, l'article 18/7 de la Loi R&S établit quant à lui également une distinction entre « *intercepter* » des communications électroniques et « *en prendre connaissance* », et se réfère de manière générale à la nécessité de la collaboration d'un opérateur ou fournisseur de services de communications électroniques dans ce contexte (sans viser l'une ou l'autre des opérations de traitement).

21. **Deuxièmement**, le demandeur indique que la coopération au déchiffrement « *s'inscrit encore* ***dans la logique de « permettre l'interception » au sens technique*** » (mis en gras par l'Autorité), **sans expliquer néanmoins en quoi l'interception nécessiterait un déchiffrement et de**

quelles données. Sur ce point, une communication électronique devrait pouvoir être interceptée sans que son contenu ne soit pour autant déchiffré. **Il ne va pas de soi en termes de prévisibilité de la norme applicable, que l'interception d'une communication implique un déchiffrement et ce, de quelles données**. Le SGRS est d'ailleurs libre ensuite, une fois une communication interceptée, de chercher à l'aide des moyens et méthodes légales et techniques dont il dispose, un moyen de déchiffrer celle-ci ou de contourner à l'avenir, le chiffrement des communications entre les parties concernées. Par exemple, les considérations suivantes peuvent être reprises d'un arrêt du 13 février 2024, *Podchasov v. Russia*, Req. n° 33696/19, de la Cour EDH concernant la messagerie Telegram :

- Un extrait d'un rapport de l'Office of the United Nations High Commissioner for Human Rights précise notamment que « *Such alternative measures include improved, better-resourced traditional policing, undercover operations, metadata analysis and strengthened international police cooperation* » (considérant n° 28 de l'arrêt) ;

- Un Joint Statement d'Europol et ENISA, indique que : « […] *The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects. Moreover, forensic methods that make use of physical fingerprints of devices might not help to intercept the communication content itself, but might provide other important clues for the investigator. Even so, there are cases in which there are no such alternatives and access to the concealed content can only be gained by a form of decryption*. […] *When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised. We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found. In this respect, the deployment of European R&D instruments may drive this collaboration while at the same time EU Agencies can work closely together in establishing best practices* » (considérant n° 33 de l'arrêt) ;

- Le European Information Society Institute explique notamment que : « *EISI also submitted that less intrusive targeted alternatives to combat crime and protect national security existed, such as, among other things, using live forensics on seized devices, guessing or obtaining private keys held by parties to the communication, using vulnerabilities in the target's software*

or sending an implant to targeted devices. While indiscriminate backdoors might be cheaper for the State than alternative investigative measures, they were expensive for society at large on account of the security risks they produced. The fact that the alternative methods were significantly more difficult to use on a large scale on account of their labour intensiveness, cost and logistical complexity should be viewed positively as hurdles forcing the prioritisation and targeting of measures » (considérant n° 47 de l'arrêt).

22. Cela étant précisé, **l'Autorité observe qu'en la matière, l'état de la technique n'a pas évolué et que dans plusieurs situations, il n'est toujours pas possible de lever le chiffrement des communications électroniques sans affaiblir le niveau de fiabilité de la technique pour les utilisateurs qui ne sont pas concernés** par le déchiffrement à mettre en œuvre. A ce sujet, l'Expert désigné par l'Autorité a considéré ce qui suit :

« *Het is **belangrijk om te verduidelijken in welke mate men geëncrypteerde informatie wil decrypteren**. Op onze vraag tot verduidelijking heeft de aanvrager geantwoord dat het enkel gaat om encryptie op verbindingen tussen apparaten van de aanbieder van diensten of de operator zelf; in dit geval beschikken de aanbieder dan wel de operator over de sleutels en kunnen ze deze decrypteren. Hierbij **moet er dan wel voor gezorgd worden dat dit geen verzwakking van de beveiliging inhoudt voor andere gebruikers of dat gegevens die niet het doelwit zijn ook zouden gedecrypteerd worden. Het voorstel zou dan ook expliciet moeten vermelden dat er nooit decryptie zal gevraagd worden van informatie die "end-to-end" vercijferd is of informatie die vercijferd is in de applicatielaag**.*

*Hierbij is het belangrijk om op te merken dat **alle academische experten het erover eens zijn dat het er geen technische oplossingen bestaan die toegang geven tot geëncrypteerde gegevens zonder de bescherming die encryptie kan bieden ernstig te verzwakken**[12]. Het joint statement [13]van Europol en ENISA van 23 mei 2015 beweert dat het wel mogelijk is ("We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found"), maar 10 jaar later is er nog steeds geen technische oplossing gevonden die dit doel zelfs maar ten dele bereikt (er zijn wel een aantal systemen voorgesteld in de wetenschappelijke literatuur die proberen om dit te bereiken, maar geen enkel is effectief en haalbaar). Ook **zijn alle experten het erover eens dat de digitale maatschappij enkel***

[12]« *Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield "Whit" Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner, Keys Under Doormats. Mandating insecurity by requiring government access to all data and communications, https://cacm.acm.org/opinion/keys-under-doormats/* ».

[13] « *https://www.enisa.europa.eu/news/enisa-news/enisa-europol-issue-joint-statement* ».

> ***maar effectief kan beschermd worden als we de digitale infrastructuur beschermen met sterke encryptie*** » (mis en gras et modification de la numérotation des notes de bas de page par l'Autorité).

23. **Troisièmement**, l'Autorité souligne qu'une **très grande variété de services** sont visés par l'obligation de coopération consacrée dans l'article 44/5 de la Loi R&S. Il n'est ainsi clairement pas uniquement question des fournisseurs d'accès à Internet : sont également visés les prestataires de **services « *over-the-top* »** tels que, notamment, les fournisseurs de services mail et de messageries électroniques[14]. Pour rappel, la Loi R&S et le Projet visent « *quiconque fournit un service consistant à offrir à ses clients une possibilité d'échange électronique d'informations* ». **De telle sorte que**, d'une part, la **distinction opérée par le demandeur** entre les mesures de chiffrement mises en place par l'opérateur ou le fournisseur et les autres mesures de chiffrement, **est moins pertinente** dans un contexte où **le dispositif de la Loi R&S vise à la fois les différentes couches de services**. Et d'autre part, le dispositif de la Loi R&S pourrait en conséquence **avoir un impact plus important sur l'éventuel affaiblissement du chiffrement dans le domaine des communications électroniques**, de manière générale.

24. **Quatrièmement** en relation avec le point précédent, **ni le dispositif normatif prévu par la Loi R&S**, **ni les informations complémentaires communiquées par le demandeur ne permettent de déterminer l'impact** qu'est susceptible d'avoir la coopération au déchiffrement **sur les propriétés de la technologie de chiffrement des communications des utilisateurs des services concernés *en général*** (c'est-à-dire, l'impact sur les autres utilisateurs qui ne sont pas concernés par les missions du SGRS). Autrement dit, la coopération envisagée peut-elle (doit-elle) être limitée à la mise en œuvre de mesures qui n'ont pas un impact sur la fiabilité du chiffrement mis en place pour les communications des utilisateurs dont les communications ne sont pas interceptées, ou celle-ci est-elle susceptible d'affaiblir de manière générale, en rendant plus vulnérable (à l'égard d'acteurs légitimes), la technologie de chiffrement utilisée ? **Il s'agit ici d'un point fondamental qui a également été soulevé par l'Expert désigné par l'Autorité[15]**. Notamment, l'Autorité souhaite évoquer les considérants nos 77-78 de l'arrêt du 13 février 2024, Podchasov v. Russia, Req. n° 33696/19, dans lequel la Cour EDH a jugé ce qui suit :

> « *77. As noted above (see paragraph 57 above), it appears that in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's "secret chats", it would be necessary* ***to weaken encryption for all users****. These*

[14] Voir les considérants nos 13-16.

[15] Voir le considérant n° 22.

measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field (see, in particular, paragraphs 28 and 34 above).

78. The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations (see Yüksel Yalçınkaya v. Türkiye [GC], no. 15669/20, § 312, 26 September 2023). However, ***it takes note in this connection of the calls for alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution****" (see, on the possibilities of alternative methods of investigation, the Joint Statement by Europol and the European Union Agency for Cybersecurity, cited in paragraph 33 above, and paragraph 24 of the Report on the right to privacy in the digital age by the Office of the United Nations High Commissioner for Human Rights, cited in paragraph 28 above; see also the explanation by third-party interveners in paragraph 47 above).*

79. The Court concludes that ***in the present case the ICO's statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued*** » (mis en gras par l'Autorité).

25. **Cinquièmement** enfin, l'Autorité se réfère de manière générale à son récent **Avis n° 16/2025 du 27 mars 2025** ***d'initiative relatif à la Convention des Nations-Unies contre la cybercriminalité*** *(CO-A-2025-019)*, dans lequel notamment, au considérant n° 23, elle préconise de **saisir la Cour de Justice** afin que celle-ci **rende un avis** à propos de la compatibilité avec les Traités européens de l'article 28, 4., de la Convention des Nations Unies contre la cybercriminalité[16], qui concerne

[16] Voir https://docs.un.org/A/RES/79/243, dernièrement consulté le 16/09/2025.

également la problématique en cause[17]. Et elle insiste de nouveau[18], sur **l'importance de sauvegarder le chiffrement**. Comme l'a notamment exprimé le European Data Protection Board : « *the EDPB stresses again* [EDPB-EDPS Joint Opinion 4/2022 and EPDB Statement 1/2024] *that encryption is* ***essential for ensuring the security and confidentiality of personal data and electronic communications****, as it provides strong technical safeguards against access to that information by anyone other than the user and the recipients chosen by him, including by the provider. In particular, in the context of interpersonal communications, genuine end-to-end encryption ('E2EE') covering the terminal devices and the data therein, with the decryption keys held solely by the users is a crucial tool for ensuring the confidentiality of electronic communications.* ***Preventing the use of encryption or weakening the effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide*** »[19] (mis en gras par l'Autorité).

26. Enfin, dans ses réponses à la troisième demande d'informations complémentaires adressée par l'Autorité, le demandeur a précisé ce qui suit :

> « *Le concours de l'opérateur/fournisseur pour la levée du chiffrement éventuellement appliqué ne se fera que dans le cas où ce chiffrement est réalisé par le fournisseur ou l'opérateur lui-même (exemple : chiffrement des liaisons entre les équipements du fournisseur ou de l'opérateur lui-même).* ***Le concours de l'opérateur ou du fournisseur ne sera jamais demandé pour déchiffrer des communications chiffrées de bout en bout ou au niveau applicatif****. Il est par ailleurs clair que pour les communications chiffrées, les données qui seront disponibles pour les agents du SGRS après le double filtrage seront limitées à des*

---

[17] Cette disposition est rédigée comme suit :

« *Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système d'information et de communication en question, du réseau d'information et de télécommunications, ou de leurs éléments constitutifs, ou des mesures appliquées pour protéger les données électroniques qu'ils contiennent, de fournir, dans la mesure du raisonnable, toutes les informations nécessaires pour permettre l'application des mesures visées aux paragraphes 1 à 3 du présent article* ».

En substance, sans entrer dans le détail de ces dispositions, le 1. du même article vise la perquisition informatique, le 2. l'extension de celle-ci et le 3., la saisie de systèmes informatiques et copie de données électroniques.

[18] Voir encore l'Avis n° 69/2025 du 26 août 2025 *concernant la « Nationale Cybersecurity Strategie 3.0, 2026-2030 » (CO-A-2025-108)*, considérant n° 21.

[19] EDPB, « Statement 5/2024 on the Recommendations of the Hight-Level Group on Access to Data for Effective Law Enforcement », adopté le 4 novembre 2024, point n° 3, disponible sur https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf, dernièrement consulté le 30/07/2025. Plus récemment, voir encore EDPS, Opinion 23/2025 on the two Proposals for Council Decisions on the signing and conclusion of the United Nations Convention against Cybercrime, disponible sur https://www.edps.europa.eu/system/files/2025-09/25-09-04_opinion_united_nations_convention_against_cybercrime_en.pdf, dernièrement consulté le 20/10/2025, considérant n° 48 :

« *In the digital age, technical solutions to secure and protect the confidentiality of electronic communications, including measures for encryption, are key to ensure the enjoyment of all fundamental rights*[…]. *The EDPS therefore calls on Member States to carefully consider the potential impact, in particular on fundamental rights and cybersecurity, of any measures that might result in the weakening or degrading of encryption*[…]. *In particular, Member States should abstain from imposing any obligations that would weaken data security for all users of an electronic communications service* ».

métadonnées uniquement. Si un accès au contenu est requis ou bien qu'une identification d'adresse IP s'avère nécessaire, il sera fait appel pour ces hypothèses à d'autres méthodes de collecte de données décrites dans la loi organique » (mis en gras par l'Autorité).

27. Dans ces conditions, l'Autorité constate tout d'abord que **le dispositif du Projet ne prévoit pas d'obligation de coopération des opérateurs et fournisseurs de communications électroniques au déchiffrement** des communications électroniques *in fine* concernées par les interceptions.

28. Si l'auteur du Projet a l'intention de prévoir cette coopération, **il lui incombe d'adapter le dispositif du Projet, en prenant en considérations les développements précédents**. A cet égard, il conviendra de prévoir explicitement dans le dispositif du Projet à tout le moins :

- Que premièrement, la coopération au déchiffrement des communications électroniques concernées **ne concerne que la solution technique de chiffrement mise en œuvre par l'opérateur ou le fournisseur de service de communications électronique sollicité lui-même** ;

- Que deuxièmement, cette coopération **ne peut pas avoir pour effet de diminuer la qualité de la solution technique de chiffrement choisie par cet opérateur ou fournisseur, pour les autres utilisateurs dont les communications électroniques ne doivent pas être interceptées**. En d'autres termes, l'obligation de coopération des prestataires de services concerné ne peut pas avoir un effet sur le niveau et la qualité de la solution technique de chiffrement que ceux-ci offrent aux utilisateurs dont les communications ne doivent pas être interceptées. **S'il n'existe pas de solution disponible compte-tenu de la technique de chiffrement choisie par l'opérateur ou le fournisseur de service de communications électroniques, la coopération ne pourra donc pas être mise en œuvre** ;

- Et enfin que troisièmement, comme l'a indiqué le demandeur, **le concours de l'opérateur ou du fournisseur ne peut pas être demandé pour déchiffrer des communications chiffrées de bout en bout ou au niveau applicatif**.

29. Cela état précisé, ce questionnement est à prendre en compte dans la recommandation générale de l'Autorité de **mener un débat parlementaire actualisé à propos des articles 44 et 44/5 de la Loi R&S[20]**.

[20] Voir le considérants n° 69.

II.2.4. Interactions avec le droit international public

30. Dans deux de ses avis, **le Conseil d'Etat soulève un problème de droit international lié à la Loi R&S dans le contexte du présent avis[21]**. L'Autorité a interrogé le demandeur quant à la question de savoir comment ce problème était résolu lorsque la collaboration sollicitée implique des communications électroniques qui ont lieu exclusivement en-dehors de la juridiction de la Belgique[22] ? Le demandeur a répondu ce qui suit :

> « *Bien que les institutions/organisations des listes n'impliquent pas d'office des résidents belges et/ou des services utilisés depuis la Belgique, les activités desdites institutions/organisations ont un lien direct avec les intérêts protégés par le SGRS explicités dans ses missions de l'article 11, §1er de la loi organique.*
> *Ensuite, à ce jour, le droit international ne contient pas de disposition claire interdisant les interceptions de communications électroniques opérées à partir du territoire d'un État et visant des communications entre personnes situées en dehors de sa juridiction, notamment dans le cadre de missions de renseignement liées à la sécurité nationale.*
> *Bien que certains principes généraux du droit international soient susceptibles d'être invoqués (notamment le respect de la souveraineté des États, la non-ingérence dans les affaires intérieures, ou la protection de la vie privée) leur application concrète au cyberespace, et en particulier aux interceptions extraterritoriales opérées à des fins de renseignement, fait encore l'objet de débats au niveau international. À ce stade, aucun consensus juridique ne permet d'affirmer que ce type d'interception est interdit par le droit international* ».

31. L'Autorité prend acte de cette explication. **Il appartient au Conseil d'Etat de se prononcer à ce sujet**, **et selon ses conclusions, il incombe à l'auteur du Projet d'en tirer les conséquences sur le plan de la licéité des traitements de données envisagés**. L'évaluation du Projet au regard du droit international public est d'autant plus importante que son champ d'application est large.

II.3. Régime de contrôle spécifique de l'interception et extranéité de la situation concernée

32. L'Autorité a recherché dans l'exposé des motifs de la Loi de 2017 les **raisons susceptibles de motiver la mise en place d'un régime juridique *ad hoc* et moins contraignant concernant le**

---

[21] Voir en particulier Avis du Conseil d'Etat n° 32.623/4 du 28 janvier 2002, *concernant un avant-projet de loi 'modifiant l'article 44 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité'*, pp. 3-7.

[22] Par exemple, un échange de courriels via Hotmail concernant des personnes A et B qui ne sont pas résidentes belges et n'utilisent pas les services d'Hotmail depuis la Belgique, mais qui sont bien impliquées dans les activités d'une organisation visée par la liste.

contrôle du SGRS dans l'interception des communications électroniques **émises ou reçues à l'étranger**.

33. Bien qu'il n'apparaisse plus nécessaire de le souligner[23], l'Autorité souhaite néanmoins rappeler que conformément à l'article 1er de la CEDH, les **droits consacrés par la CEDH** ne sont pas uniquement applicables sur le territoire belge. En effet, ils **s'appliquent plus largement à toute personne relevant** de la juridiction belge, soit **de l'exercice de ses compétences par la Belgique**[24].

34. L'exposé des motifs indique ce qui suit s'agissant de l'intrusion dans les systèmes informatiques[25] : « *Les procédures actuellement fixées pour mettre en œuvre une méthode exceptionnelle lors d'opérations à l'étranger ne sont pas toujours praticables puisque, encore plus à l'étranger, le besoin en renseignement (art. 11, § 1er, 1°) et en sécurité (art. 11, § 1er, 2°) est immédiat et ne peut pas toujours attendre, même quelques heures, que la procédure d'extrême urgence soit suivie, la menace n'étant pas potentielle mais concrète et imminente. Les décalages horaires ne facilitent pas les choses. Et surtout, les communications vers la Belgique ne sont pas toujours possibles, ni même sécurisées. En outre, il est parfois très difficile d'identifier une cible précise* »[26].

35. Plus généralement, et cette fois **s'agissant des prérogatives du SGRS à l'étranger, l'exposé des motifs de la Loi de 2017 indique aussi ce qui suit**[27] : « *Dans le cadre de certaines opérations, alors qu'il est indispensable de collecter des informations,* ***le SGRS n'est pas en mesure de suivre la procédure fixée pour recourir aux méthodes spécifiques et exceptionnelles pour différentes raisons: à l'étranger, décalage horaire, urgence, aucun moyen de communication sécurisé, impossibilité de cibler une personne ou un événement précis,*** *… Par conséquent, il convient de* ***prévoir une plus grande flexibilité pour certaines manières de collecter des informations****, tout en maintenant un contrôle sur la collecte* »[28] (mis en gras par l'Autorité).

---

[23] Le Conseil d'Etat avait soulevé ce point il y a longtemps, voir l'Avis du Conseil d'Etat n° 32.623/4 du 28 janvier 2002 *concernant un avant-projet de loi 'modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité'*, p. 8.

[24] Notamment, voir Cour Européenne des Droits de l'Homme, « Fiche thématique – Juridiction extraterritoriale des Etats parties », juillet 2018, disponible sur https://www.echr.coe.int/documents/d/echr/fs_extra-territorial_jurisdiction_fra, dernièrement consulté le 16/09/2025.

[25] Interrogé dans ce contexte, le demandeur a attiré l'attention de l'Autorité sur le fait que ce passage visait bien l'intrusion dans les systèmes informatiques et pas l'interception des communications électroniques.

[26] *Doc. Parl.*, Ch. des Représentants, n° 54-2043/001, p. 84.

[27] *Doc. Parl.*, Ch. des Représentants, n° 54-2043/001, p. 7.

[28] Et l'exposé des motifs poursuit :

Actuellement, le SGRS peut intercepter des communications émises à l'étranger selon un plan d'écoute annuel énumérant la liste des organisations et institutions qui feront l'objet d'interceptions, plan approuvé par le ministre de la Défense et transmis au Comité R.

Il est proposé d'utiliser la même procédure pour l'intrusion dans un système informatique situé à l'étranger et la prise d'images à l'étranger, sur la base d'un plan annuel d'intrusions et de prises d'images.

Cela permettra, par exemple, au SGRS de s'introduire immédiatement dans le GSM d'un kamikaze situé à l'étranger pour vérifier qu'il ne planifie pas l'explosion d'un engin, à condition que ce kamikaze appartienne à une organisation visée dans le plan annuel

36. **L'hypothèse visée dans le cadre du Projet semble cependant différente** dès lors qu'elle nécessite des communications écrites entre le SGRS et les fournisseurs de services de communications électroniques et opérateurs et même l'installation d'équipements « chez » ces prestataires. Concrètement d'ailleurs, les interceptions auront lieu en Belgique à tout le moins lorsque l'opérateur ou le fournisseur se trouve en Belgique, mais encore lorsqu'une infrastructure technique est utilisée en Belgique[29].

37. Dans ce contexte d'ailleurs, **l'identification claire de la portée territoriale de l'article 44 est malaisée**. L'Autorité a interrogé le demandeur **afin qu'il identifie quel élément d'extranéité est requis du point de vue des activités du SGRS, pour que les articles 44 et 44/5 s'appliquent**. A la lecture de ces dispositions, il n'apparaît pas nécessaire qu'un agent du SGRS soit présent physiquement dans la zone géographique dans laquelle se trouve l'organisation ou l'institution concernée, pour que ces dispositions puissent s'appliquer. Le SGRS pourra-t-il obtenir les communications électroniques vers et depuis un pays étranger C, lorsqu'une organisation ou une institution d'intérêt s'y trouve, nonobstant l'absence d'opération physique du SGRS sur place, pour autant que l'organisation ou l'institution concernée soit impliquée dans une menace visée à l'article 11, § 1er, 1° à 3° et 5° de la Loi R&S. ? Le demandeur a répondu ce qui suit :

> « ***C'est exact. Les éléments juridiques permettant de déclencher les articles 44 et 44/5 sont le fait que les communications sont émises ou reçues à l'étranger*** *et que celles-ci proviennent des institutions/organisations reprises dans les listes visées à l'article 44/3* » (mis en gras par l'Autorité).
>
> « *C'est bien l'idée mais pour être plus précis, le SGRS sera en mesure d'obtenir les communications si l'organisation ou l'institution concernée fait bien partie des listes visées à l'article 44/3 de la loi organique. Ces listes sont approuvées annuellement selon la procédure décrite à l'article 44/3 précité et elles justifient pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°* ».

38. **Au regard de ces éléments, l'Autorité se pose la question de savoir comment justifier**, dans le contexte du Projet, que les interceptions mises en œuvre par le SGRS **ne soient pas soumises aux garanties naturelles applicables aux méthodes exceptionnelles de recueil de renseignements** (cf. la méthode de l'article 18/17 de la Loi R&S, nécessitant notamment une autorisation

[29] Voir la réponse communiquée par le demandeur et citée au considérant n° 16 (« *Les communications faisant l'objet de la coopération entre le fournisseur ou opérateur et le SGRS seraient dans ce cas rapatriées jusqu'aux installation situées en Belgique* »).

préalable de la Commission BIM). L'Autorité a interrogé le demandeur et celui-ci a communiqué les informations complémentaires suivantes :

> « *Avant de répondre à cette question, il est important de noter que la finalité du projet d'arrêté royal est de fixer les modalités du concours de l'opérateur/fournisseur. Le projet d'arrêté royal ne fixe pas une nouvelle méthode d'interception de données, celle-ci étant déjà possible et encadrée par les articles 44 et 44/3 de la loi du 30 novembre 1998.* ***Les exemples mentionnés dans l'exposé des motifs*** *de la loi de 2017* ***ne sont pas limitatifs et ne se rapportent pas tous à l'article 44. D'autres situations, menées à distance par le SGRS, peuvent justifier un cadre plus souple*** *que celui imposé par les méthodes exceptionnelles. En effet, il n'est* ***pas toujours possible d'évaluer à l'avance le degré de gravité (potentiel) d'une menace étrangère, ni d'anticiper si les conditions légales strictes permettant de recourir à une méthode exceptionnelle sont remplies****. En conclusion, le chapitre V susvisé a été conçu pour répondre aux besoins spécifiques du renseignement à l'étranger,* ***notamment dans des contextes où l'application du régime des méthodes exceptionnelles (et notamment le contrôle préalable par la Commission BIM) ne serait pas opérationnellement viable et ce, indépendamment de la présence effective du SGRS sur le terrain*** » (mis en gras par l'Autorité).

39. **L'Autorité prend acte de cette explication qui toutefois, ne la convainc pas de manière décisive**. La justification énoncée par le demandeur ne permet effectivement pas de comprendre concrètement en quoi le régime de contrôle des méthodes exceptionnelles de recueil de données est inadapté dans les situations visées par le Projet. **Compte-tenu de l'expérience approfondie du Comité R et de sa meilleure information en la matière, l'Autorité choisit de s'en remettre à la position qu'exprimerait celui-ci quant à l'éventuelle nécessité de créer et modaliser un contrôle *ad hoc*** (distinct du contrôle normal des méthodes exceptionnelles de renseignement), et est en outre d'avis **que la motivation du cadre légal actuel doit impérativement être étayée**. **En l'état, l'Autorité ne dispose pas des informations nécessaires pour se prononcer.**

40. Dans tous les cas, si le Comité R estime que les interceptions et coopérations concernées ne justifient pas un mode de contrôle *ad hoc* moins protecteur, il conviendra d'en tirer les conclusions quant à la licéité des traitements imposés aux opérateurs et fournisseurs de services de communications électroniques.

41. Ceci est sans préjudice du fait qu'il **relève bien de la compétence de l'Autorité d'évaluer la conformité au droit applicable du concours exigé des opérateurs et fournisseurs de ser-**

vices de communications électroniques dans le cadre de ces activités de prestation de services[30] (remarque : juridiquement toute autre est la situation dans laquelle le SGRS, lui-même, agirait à l'insu et sans le concours d'un opérateur ou d'un fournisseur de communications électronique[31]). Autrement dit, l'Autorité doit se positionner sur l'éventuelle absence de garanties appropriées dans ce contexte.

42. Dans ce cadre, elle a interrogé le demandeur quant à la justification de l'article 44 de la Loi R&S au regard de la **jurisprudence de la CJUE dans le domaine des dérogations à la confidentialité des communications électroniques**[32] (notamment, dans le cadre du contrôle *ad hoc*, le Comité R ne doit pas autoriser l'accès aux données concernées, et en outre, les listes prévoient plus un programme général d'interception qu'une liste concrète de communications à intercepter). Le demandeur a répondu ce qui suit :

> « *Les seules communications qui peuvent être interceptées sont celles **relatives aux institutions/organisations des listes** visées à l'article 44/3 de la loi organique. Par conséquent, les listes ne prévoient pas un programme général d'interception mais bien une **liste ciblée d'organisations et institutions**.*
> *Conformément à l'article 44/3 précité, **le Comité R dispose d'un contrôle avant**, pendant et après les interceptions qui sont effectuées.*
> *En ce qui concerne le contrôle « avant » les interceptions, **les listes de l'article 44/3 sont approuvées par le Ministre de la Défense et sont également envoyées au Comité R.** Dans son rôle d'autorité de contrôle des activités du SGRS, le Comité R peut, à tout moment, émettre des objections par rapport à ces listes, stopper les interceptions et ordonner la destruction des données recueillies.*

---

[30] Sur ce point, « *conformément à la jurisprudence constante de la Cour* [de justice], *bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit [voir, en ce sens, arrêts du 4 juin 2013, ZZ, C-300/11, EU:C:2013:363, point 38 et jurisprudence citée ; du 20 mars 2018, Commission/Autriche (Imprimerie d'État), C-187/16, EU:C:2018:194, points 75 et 76, ainsi que du 2 avril 2020, Commission/Pologne, Hongrie et République tchèque (Mécanisme temporaire de relocalisation de demandeurs de protection internationale), C-715/17, C-718/17 et C-719/17, EU:C:2020:257, points 143 et 170]* » C.J.U.E. (Gr. Ch.), arrêt du 6 octobre 2020, Privacy International, aff. C-623/17, considérant n° 44. Voir également C.J.U.E. (Gr. Ch.), arrêt du 6 octobre 2020, Quadrature du Net, affs jointes C-511/18, C-512/18 et C-520/18, considérants nos 87-104.

[31] Voir également le considérant n° 70.

[32] Notamment à ce sujet, voir les arrêts suivants : C.J.U.E. (Gr. Ch.), arrêt du 20 septembre 2022, Bundesrepublic Deutschland c/ SpaceNet AG, Telekom Deutschland GmbH, affs jointes C-793/19 et C-794/19 ; C.J.U.E. (Gr. Ch.), arrêt du 5 avril 2022, G.D. c/ Commissionner of An GardaSiochana et al., aff. C-140/20 ; C.J.U.E. (Gr. Ch.), arrêt du 6 octobre 2020, La Quadrature du Net, affs jointes C-511/18, C-512/18 et C-520/18 ; C.J.U.E. (Gr. Ch.), arrêt du 21 décembre 2016, Tele2 Sverige, affs jointes C-203/15 et C-698/15 ; C.J.U.E. (Gr. Ch.), arrêt du 8 avril 2014, Digital Rights Ireland, affs jointes C-293/12 et C-594/12.

Voir également C.J.U.E. (Gr. Ch.), arrêt du 6 octobre 2020, Privacy International, aff. C-623/17, en particulier, les considérants nos 61 et 76 (et la jurisprudence citée aux considérants nos 65, 67-68) ; C.J.U.E. (troisième chambre), arrêt du 16 février 2023, HYA, IP, DD, ZI, ET SS, aff. C-349/21. 162/22

Par conséquent, le Comité R dispose bien d'un contrôle préalable en la matière, celui-ci découlant tant des modalités de contrôle décrites à l'article 44/3 que des compétences générales du Comité en tant qu'autorité de contrôle du SGRS » (mis en gras par l'Autorité).

43. L'Autorité prend acte de cette explication. Cependant, sans préjudice des développements du considérant n° 39, en particulier compte-tenu de l'ingérence importante causée par les articles 44 et 44/5 de la Loi R&S, **l'Autorité ne voit pas sur quelle base**, à l'aune de la jurisprudence européenne précitée[33], **il serait justifiable de dispenser le SGRS d'une décision (autorisation) préalable de la Commission BIM (ou du Comité Permanent R), sauf cas d'urgence**, comme cela est prévu dans le cadre du recours aux méthodes exceptionnelles de recueil de données.

44. Dans une hypothèse telle que celle en cause dans le présent avis (à savoir l'interception de communications électroniques par un service de renseignement), **les garanties procédurales de ce type sont d'autant plus importantes** vu qu'il n'est pas toujours possible d'identifier avec précision les catégories de données qui seront traitées dans la législation applicable. L'Autorité a déjà mis en évidence que, s'agissant des autorités judiciaires pénales et de services de contrôle/d'inspection, les éléments essentiels des traitements de données à caractère personnel prévus (dont les catégories de données) et leur proportionnalité découleront généralement d'une lecture combinée des règles dont elles assurent le respect ainsi que des pouvoirs que le droit leur attribue, y compris les limites et les garanties procédurales qu'il consacre[34].

45. Et encore, l'Autorité est d'avis que le dispositif prévu par le Projet **entraîne en réalité**, au niveau des opérateurs ou fournisseurs de services de communications électroniques concernés et **à l'égard des utilisateurs concernés** par la sélection de flux mise en place, une **prise de décision fondée exclusivement sur un traitement automatisé de données impliquant un profilage** qui produit des **effets juridiques les concernant et les affecte de manière significative** dès lors que leurs flux de communications sont communiqués à un service de renseignements en vue d'être traités par celui-ci, notamment dans un contexte normatif où leurs droits sont limités conformément au droit national. Sur ce point, l'article **22 du RGDP** nécessite la mise en place de mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes des personnes concernées.

46. Enfin, concernant **l'article 19 du projet** qui confie une mission de **contrôle au Comité R**, il convient de faire échos dans le présent Avis au **considérant n° 13 de l'Avis du Comité R** selon lequel, notamment :

---

[33] Voir la note de bas de page n° 32.

[34] Voir l'Avis n° 129/2022 du 1er juillet 2022 concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie (CO-A-2022-110) ; et l'Avis n° 252/2022 du 1er décembre 2022 *concernant un avant-projet de loi portant réforme du Livre II du Code pénal (CO-A-2022-281)*, considérant n° 9.

« *L'article 19 confère au Comité une mission de contrôle de la coopération entre le SGRS et l'opérateur du réseau ou le fournisseur de services concerné. Ce contrôle particulier comporte trois volets. Tout d'abord, le Comité est chargé d'émettre un avis dans le cadre de la conclusion d'un accord de coopération donné. Le Comité dispose d'un délai de deux semaines accordé par l'auteur du Projet pour rendre cet avis. Deuxièmement, le Comité est chargé de contrôler la mise en œuvre du présent accord de coopération. Enfin, le Comité doit effectuer des contrôles périodiques de la mise en œuvre au moyen du mécanisme de révision visé à l'article 18.*

En ce qui concerne le contrôle a priori, ***le Comité estime que deux semaines***[35] ***ne suffisent pas pour rendre un avis fondé, compte tenu du caractère hautement technique de la coopération entre le SGRS et l'opérateur du réseau ou le fournisseur de services concerné. Le Comité souhaite en outre que le Projet prévoie une obligation pour le SGRS de lui fournir des explications orales****.*

En ce qui concerne le contrôle périodique prévu, ***le Comité ne comprend pas bien quel type de contrôle est attendu par l'auteur****. Le dispositif n'est pas très clair à ce sujet et le rapport au Roi ne fournit pas d'explications supplémentaires à ce sujet.*
Enfin, il convient de noter que ***la mise en place d'une mission de contrôle particulière au sein du Comité sollicitera davantage les capacités de celui-ci. Afin de permettre au Comité de répondre de manière adéquate aux attentes et aux besoins du gouvernement en matière de contrôle, il doit disposer de ressources matérielles, financières et humaines suffisantes****. Le Comité demande que cet aspect soit pris en considération lors de l'approbation du projet d'arrêté royal* » (mis en gras par l'Autorité).

47. L'Autorité rejoint la position du Comité R. **A défaut de prise en considération de l'Avis du Comité R sur ce point, l'auteur du Projet risque de consacrer un contrôle de façade à l'efficacité douteuse**. Ceci est d'autant plus important compte-tenu du secret entourant les activités du SGRS que seul le Comité R peut partager.

II.4. Le dispositif mis en place par le Projet, sur la base de la Loi R&S

II.4.1. Le Projet et la Loi R&S

48. Avant tout, l'Autorité observe que l'opérateur ou le fournisseur de service de communications électroniques concernés est **obligé de conclure un accord de coopération avec le SGRS**, et **à défaut**

[35] Le délai prévu par le Projet est plus précisément de « *quatorze jours ouvrables à dater de l'envoi de la réquisition* ». Ce qui ne change rien au commentaire émis par le Comité R.

d'accord, deux ministres pourront fixer les termes de la coopération envisagée. Plus précisément, l'accord de coopération « *complète les modalités de coopération génériques décrites dans les articles 11 à 17* [du Projet] *et reprend au minimum les dispositions détaillées sur le plan technique, organisationnel et financier* »[36]. Le prestataire de service concerné et le SGRS disposent d'un délai de 9 mois pour conclure cet accord. A défaut d'accord endéans ce délai, à la demande d'une des parties, « *le ministre de la Défense et le ministre des Télécommunications fixent conjointement dans un délai de 3 mois* […], *par voie de décision ministérielle, les modalités de la coopération* »[37].

49. **L'article 14 du Projet**, au cœur du dispositif envisagé, est rédigé comme suit :

> « ***Le fournisseur*** *d'un service de communications électroniques* ***ou l'opérateur*** *du réseau* ***met en place un système technique*** *garantissant la* ***transmission automatique des flux de données et de métadonnées*** *de communications* ***émises ou reçues à l'étranger vers les équipements du SGRS*** *mis* ***en place chez le fournisseur*** *d'un service de communications électroniques* ***ou l'opérateur*** *du réseau.*
>
> *Les* ***équipements*** *mentionnés à l'alinéa 1er assurent la* ***fonction de filtres techniques*** *afin* ***de n'intercepter que des flux*** *de données et de métadonnées de* ***communications émises ou reçues dans des zones géographiques où se trouvent des institutions et organisations qui font partie des listes*** *visées à l'article 44/3 de la loi du 30 novembre 1998 et en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5° de ladite loi* » (mis en gras et souligné par l'Autorité).

50. Cette disposition prévoit la mise en place de **deux solutions techniques,** qui semblent **sous des responsabilités distinctes (opérateur ou fournisseur/SGRS)**. L'opérateur ou fournisseur est chargé de mettre en place sur son infrastructure « ***un système technique*** », sous sa responsabilité, de sélection des communications électroniques et de transmission de celles-ci vers « ***les équipements du SGRS mis en place chez le*** » fournisseur ou opérateur concerné, relevant de la responsabilité exclusive du SGRS (mise en œuvre d'un **filtrage** afin d'identifier les données de communications électroniques concrètement nécessaires à l'exercice de la mission concernée du SGRS).

51. Cependant, ce dispositif soulève plusieurs questions qui ont été adressées au demandeur. **En effet notamment, la Loi R&S et le Projet ne déterminent pas les données/les critères concrets sur la base desquelles peuvent être filtrées les communications électroniques concernées au niveau de l'opérateur ou du fournisseur de service de communications électroniques**

[36] Article 9, § 1er, du Projet.

[37] Article 9, § 2, du Projet.

(soit au niveau du « **système technique** »). La Loi R&S se limite à prévoir la rédaction d'une liste annuelle comportant des organisations ou institutions faisant l'objet d'interceptions, la raison pour laquelle de telles interceptions peuvent avoir lieu ainsi que la durée de celles-ci. Et l'article 14, al. 2, du Projet n'indique comme critère de sélection que les « *zones géographiques où se trouvent des institutions et organisations qui font parties des listes* » concernées.

II.4.2. Informations complémentaires communiquées par le demandeur

52. L'Autorité a posé de nombreuses questions au demandeur à propos du filtrage concerné et des données/critères communiqués aux opérateurs dans ce contexte[38] et de la mise à jour du filtrage compte-tenu du fait que les listes « d'écoute » sont établies sur base annuelle[39]. À la suite d'une première série de réponses, elle l'a réinterrogé afin de pouvoir identifier clairement quels étaient les *input* (depuis le système de l'opérateur/du fournisseur) et *output* (vers les équipements du SGRS), en termes de données de communications électroniques, du « *système technique* » mis en place « *chez* » l'opérateur ou le fournisseur de services de communications électroniques (voir le considérant n° 51). Enfin, après désignation d'un Expert externe, l'Autorité a adressé au demandeur une troisième demande d'informations complémentaires.

53. Les éléments suivants ont notamment été communiqués par le demandeur (remarque : dans le présent avis, les passages des réponses communiquées par le demandeur qui ne sont pas cités ne le sont pas car ils ne sont pas considérés comme déterminants au regard de la question posée) :

> S'agissant du **rôle de l'opérateur/du fournisseur à l'égard du filtrage** et des filtres qui lui seraient communiqués :
>
> « […] *la* ***responsabilité du filtrage relève du SGRS uniquement****. Le projet d'arrêté royal pourrait éventuellement être explicité davantage sur ce point (notamment dans le rapport au Roi)* » (mis en gras et souligné par l'Autorité).

---

[38] L'Autorité a demandé au demandeur : de communiquer un extrait illustratif rendu fictif d'une liste ; d'indiquer sur la base de quelles données il va être enjoint à l'opérateur ou au fournisseur de service concernés de sélectionner les communications concernées (quels types de filtres (données de filtrage) sont communiqués à l'opérateur) (Par exemple, s'il s'agit d'intercepter des communications téléphoniques, les numéros de téléphones supposés utilisés par les institutions ou organisations concernées sont-ils communiqués ? S'il s'agit d'intercepter du trafic IP, les adresses IP supposées être utilisées par ces organisations seront-elles communiquées ? Quid dans l'hypothèse de l'interception d'e-mails ou de communications via une application mobile?) ? ; de préciser s'il s'agit d'intercepter tout le trafic depuis et vers un pays, et comment est-il établi, à l'égard de l'opérateur, que la communication concernée provient bien du périmètre géographique limité dans lequel agit l'institution ou l'organisation concernée (quid de la prise en compte dans ce contexte du recours à des intermédiaires (serveurs proxy) qui empêchent de lier une communication à sa réelle origine géographique ?).

[39] La Loi R&S et le Projet prévoient une coopération sur base annuelle (les listes étant annuelles) entre les opérateurs et fournisseurs concernés. Autrement dit en principe (c'est-à-dire, sauf hypothèse de l'interception urgente et indispensable non prévue), une seule liste de « filtres » ou « données de filtrage » est communiquée à ces fournisseurs pour l'année concernée. L'Autorité a interrogé le demandeur quant à la question de savoir comment ces informations (ces filtres) étaient mis à jour à l'égard de ces fournisseurs, dès lors qu'en pratique, les abonnements aux différents services de communications électroniques (internet, 5G, mails, chats, applications, etc.) sont susceptibles d'évoluer au cours du temps.

« ***Ces éléments seront déterminés et exécutés exclusivement par le SGRS*** *et ce, dans le cadre du contrôle du Comité R prévu dans la loi organique.* ***L'opérateur n'aura ni de vue sur les données interceptées, ni a fortiori de contrôle ou de responsabilité à cet égard****. Si ce point n'est pas clair dans l'actuel projet d'arrêté royal, il pourra être explicité dans les modifications futures.*

Le concours de l'opérateur *vise principalement à* ***mettre en place une solution technique qui permet de dupliquer les données vers les équipements du SGRS qui seront paramétrés de telle façon à n'intercepter que les communications émises ou reçues à l'étranger des organisations/institutions listées à l'article 44/3*** » (mis en gras et souligné par l'Autorité).

En ce qui concerne les **listes d'organisations/d'institutions** :

« […] *La liste d'interception pourrait reprendre, par exemple, les services de renseignement et de sécurité du pays REDLAND ; l'Administration Générale du Renseignement Militaire REDLANDAIS pourrait ainsi être listée.* […] ».

Quant à la question de savoir s'il s'agit d'intercepter tout le **trafic depuis et vers un pays,** le demandeur a renvoyé à une réponse précitée au présent considérant et a ajouté ce qui suit :

« *Voir réponse précédente : le contrôle sur ce sujet sera effectué par l'entité en charge du contrôle des activités du SGRS, à savoir le Comité R et selon le cadre juridique qui est établi à cet effet (notamment la loi organique, la loi vie privée, et la loi propre au Comité R du 18 juillet 1991). A titre informatif, vous trouverez ci-dessous des* ***exemples de paramètres de filtrage envisageable*** *(liste non exhaustive), en fonction du type de fournisseur et du type de coopération envisagée :*

- *codes pays ou préfixes régionaux (opérateur téléphonique),*
- *adresses IP ou d'information de routage Border Gateway Protocol (fournisseur de service de type ISP),*
- *en ciblant exclusivement des interconnexions spécifiques d'intérêt (fournisseur de service de connexions optiques).*

La problématique de l'utilisation de VPN et d'autres solutions techniques pour camoufler la localisation exacte de l'origine d'une communication IP est bien connue du SGRS mais ne représente pas une limitation suffisante pour ne pas requérir le concours d'opérateurs ou de

fournisseurs vu qu'elle ne s'applique qu'à certains types de coopération et qu'à un nombre d'organisation limité » (mis en gras par l'Autorité).

Quant à la coopération sur base annuelle via une demande générale reprenant une liste, des opérateurs/fournisseurs, **et à propos de la mise à jour de ces listes** :

« […] *Plus précisément,* ***le concours de l'opérateur ou fournisseur consiste,*** *non pas en un traitement actif ou une analyse des communications, mais* ***en la mise en place d'un mécanisme technique qui permet de dupliquer certains flux de données*** *(communications électroniques émises ou reçues à l'étranger)* ***vers les équipements sécurisés du SGRS installés dans ses infrastructures****.*
Ces équipements sont intégralement paramétrés par le SGRS, qui assure seul la mise en œuvre du filtrage *conforme à la liste des cibles définies à l'article 44/3.* ***L'opérateur/fournisseur ne dispose*** *ni de l'accès aux données interceptées, ni d'un droit ou devoir de contrôle sur le contenu ou la portée de l'interception. Le rôle de l'opérateur est donc strictement passif et technique.*
Cette distinction est essentielle au regard de la jurisprudence de la CJUE, notamment dans l'arrêt Privacy International *(C-623/17), qui interdit aux États membres d'imposer aux opérateurs une obligation de conservation ou de transmission généralisée et indifférenciée de données de communications électroniques. Le projet d'arrêté royal respecte cette exigence, en ce qu'il ne prévoit pas une collecte massive sans discrimination, mais bien une interception ciblée, soumise à un encadrement légal, administratif et juridictionnel strict, et contrôlée par le Comité R, conformément aux exigences de la loi organique.*
S'il apparaît nécessaire de clarifier davantage ce point dans le texte de l'arrêté royal ou dans le rapport au Roi, cela pourra être envisagé dans les modifications futures du projet en question ».
« *La mise à jour et la configuration des filtres sont une responsabilité du SGRS. Ceci pourrait être explicité davantage dans le projet d'arrêté royal* » (mis en gras par l'Autorité).

54. S'agissant de la deuxième série d'interrogations adressées au demandeur, et des réponses communiquées dans ce contexte :

Quant aux **données auxquelles a accès le système technique mis en place par l'opérateur/le fournisseur**[40] :

[40] Est-il exact que le « système technique » mis en place par l'opérateur/fournisseur a accès à toutes les données (métadonnées et contenu) relatives à toutes les communications électroniques transitant par le service concerné ? Si non, qu'en est-il ?

« *Le « système technique » mis en place par l'opérateur/fournisseur aura pour but de* ***dupliquer toutes les communications électroniques spécifiques au service faisant l'objet de la coopération (par exemple, fibre optique spécifique, lien spécifique, etc).***
[…] *Cette coopération* ***ciblera cependant déjà spécifiquement certains types de communications*** *(l'objet de la coopération pourrait, par exemple, ne concerner qu'une seule et unique fibre optique dont l'origine ou la destination (à l'étranger) présente un intérêt spécifique pour l'accomplissement des missions susmentionnées du SGRS).* […] ».

A propos de **l'*input* reçu par le système de filtrage mis en œuvre sur l'infrastructure du SGRS**[41] :

« *Pour éviter les problèmes de rétention, stockage et destruction de données chez le fournisseur/opérateur,* ***l'envoi se passera en un seul temps et concernera l'entièreté des données de communications électroniques spécifiquement demandées*** *via réquisition et détaillées dans l'accord de coopération.* ***Ces données seront ensuite filtrées en deux temps (PASS / DISCARD),*** *sur la base des listes visées à l'Art 44/3 de la loi organique. Un* ***premier filtrage, plus grossier et non classifié, aura lieu chez le fournisseur de service (soft filtering) et un second filtrage, encore plus particulier et classifié, aura lieu au sein de l'infrastructure du SGRS****. A l'issue de ce second filtrage, une évaluation de la pertinence (humaine) sera effectuée et seules les données considérées comme pertinentes seront conservées* » (mis en gras et souligné par l'Autorité).

Quant au **paramétrage des systèmes techniques** mis en place par l'opérateur/le fournisseur et **quant à leur nature**[42] :

« *Les systèmes techniques mis en place par le fournisseur/opérateur* ***ne nécessitent à priori pas de paramétrage spécifique****.* ***C'est l'emplacement précis*** *de ces « systèmes techniques »* ***sur l'architecture*** *du fournisseur ou de l'opérateur qui devra être décidé en coopération entre le SGRS et le fournisseur de service ou opérateur afin de cibler uniquement les communications faisant l'objet de la réquisition* ».

[41] Le traitement de filtrage que le SGRS réalise sur ses équipements (son infrastructures) a-t-il pour input les données de l'ensemble des communications électroniques transitant par les services de l'opérateur/du fournisseur ? Si non, qu'en est-il ? (P. ex., le système fonctionne-t-il en deux étapes, (1) envoi de toutes les métadonnées, (2) envoi ensuite des données de contenus selon un premier filtrage sur la base des métadonnées ; autre ?).

[42] Le paramétrage de ce « système technique » est-il aussi décidé par le SGRS et partant, l'opérateur n'a-t-il bien aucun contrôle à cet égard ? ; De quelle technologie est-il question quant à ce « système technique » (TAP, SPAN, NPB, autre ?)?

> « *Le choix du « système technique » se fera* ***en concertation avec le fournisseur ou opérateur****. L'objectif est de minimiser l'impact pour le fournisseur ou opérateur et* ***d'utiliser le système le plus passif*** *(l'usage de test access point sera dès lors préféré au port mirroring). Le filtrage sera par contre réalisé en 2 temps : soft filtering chez le fournisseur à l'aide, par exemple de packet brokers et hard filtering au sein de l'infrastructure classifiée du SGRS sur la base d'autre outils, applications et équipements* » (mis en gras par l'Autorité).

55. Enfin, à la suite du recours à l'Expert désigné par l'Autorité, le demandeur a été interrogé une troisième et dernière fois dans ce contexte[43]. Celui-ci a notamment répondu ce qui suit :

> « *L'arrêté royal a pour but de fixer le cadre global et les modalités d'exécution des coopérations envisagées avec les opérateurs/fournisseurs de services et n'a donc pas pour objectif de décrire les détails techniques de toutes* ***les implémentations de coopérations possibles*** *car* ***chaque opérateur/fournisseur est différent sur ce niveau*** *(d'où le besoin de conclure un accord de coopération spécifique sur les modalités qui ne peuvent pas être figées de façon immuable dans l'arrêté royal).* […]
>
> *La figure ci-dessous explique globalement le fonctionnement général des coopérations envisagées :*

[43] Il a été demandé d'indiquer, par type de service ci-après :

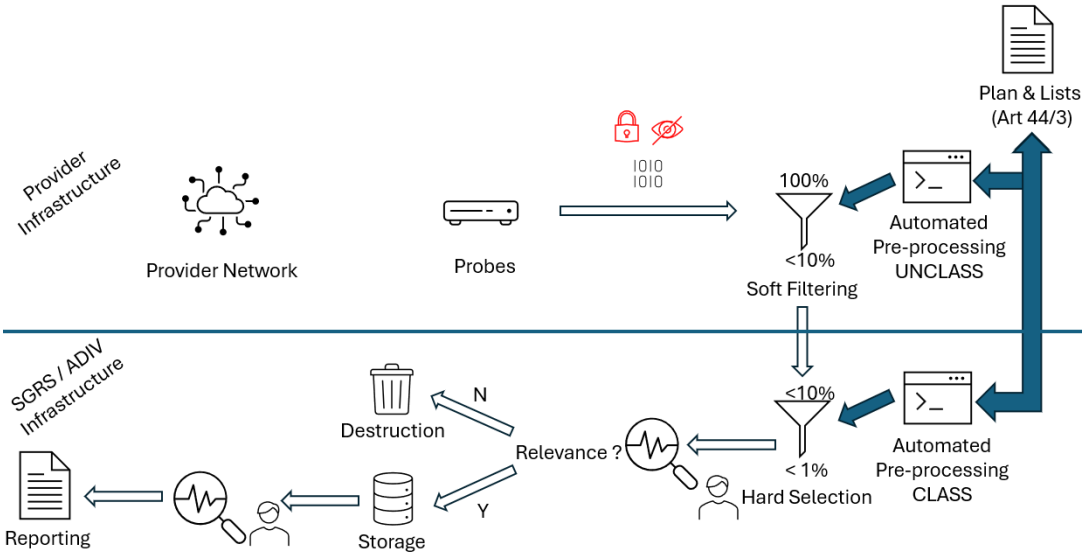
- le type de mesure/appareil technique (ou autre ? – une demande ?) qu'il est envisagé de pouvoir mettre en place, et leur capacité de filtrage, quant à l'interception des communications concernées ;
- et le type de demande quant à la levée du chiffrement éventuellement appliqué (notamment, selon les cas, s'agit-il de demander au prestataire de service de communiquer les communications déchiffrées (auquel cas le prestataire de service procède au déchiffrement – *a priori* non vu l'objectif de ne communiquer aucune information au prestataire) ou de communiquer le moyen de déchiffrement (la/les clé/s) ?),

et ce, selon que le prestataire concerné dispose ou pas de l'infrastructure pertinente sur le territoire belge ?

Concrètement, ces interrogations se posent à l'égard des types de services suivants :

- Service de communications (couche de liaison de données) ; Service d'accès à internet (IP) ; Service MPLS Multiprotocol Label Switching ; Services de téléphonie (3G-4G-4G) ; Services de communication par satellite ; Services de VPN/proxy/Tor/mixnet ;
- Service de messagerie e-mail sans chiffrement de bout en bout (type Gmail) ;
- Service de messagerie e-mail avec chiffrement de bout en bout (type Proton) ;
- Service de messagerie instantanée type Signal (conservation minimisée de métadonnées) ;
- Service de messagerie instantanée type WhatsApp (conservation plus large de métadonnées) ;
- Services de réseau social.

Enfin, l'interception comprend-elle également l'interception de messages liés au routage (BGP), aux noms de domaine (DNS) et aux autorités de certification (CA) ?



Par rapport aux différents services dont question ci-dessous, il est primordial de comprendre que ***le focus porte sur toutes les communications numériques rendues possibles via l'Internet Protocol*** *(voir également la définition indiquée dans le projet d'arrêté royal). La coopération qui sera mise en place et le concours de l'opérateur/fournisseur sont cependant complètement indépendants des couches supérieures du modèle OSI et pour les fournisseurs/opérateurs, aucune différence ne sera faite par rapport aux communications chiffrées ou non chiffrées, de type applicatives (Signal, Whatsapp, etc) ou pas.*

Les fournisseurs de service et opérateurs de réseaux auront la responsabilité d'installer des TAP (probes sur le schéma ci-dessus) dans leur architecture pour dupliquer le trafic d'intérêt *demandé par le SGRS.*

Ce trafic sera envoyé vers les équipements du SGRS qui se trouveront chez l'opérateur ou le fournisseur et qui auront pour objet d'assurer la fonction de filtre (conformément aux articles 44 et 44/3).
Le filtrage est une responsabilité du SGRS *et n'est donc pas décrit dans ce projet d'arrêté royal qui se limite aux modalités concernant le concours des opérateurs et fournisseurs de service.*
Par ailleurs, les techniques et outils utilisés sont classifiés et ne peuvent dès lors pas être détaillés dans cet e-mail ou dans un arrêté royal non classifié.

Nous vous expliquons tout de même brièvement le filtrage et le traitement envisagés dans le cadre des coopérations prévues via cet arrêté royal (ce qui suit pourrait éventuellement figurer dans le projet d'arrêté royal afin de clarifier le concours envisagé).

*Le **premier filtrage**, **automatisé** et réalisé, par exemple, au moyen de packets brokers (pass/drop), combiné ou non à d'autres équipements de filtrage, effectuera un premier filtrage **non classifié** pour isoler le trafic qui n'est pas autorisé par la loi et/ou qui n'est pas exploitable par le SGRS (**par exemple** communications chiffrées pour lesquelles seuls les premiers bytes d'une connexion chiffrée pourraient être retenus). Ce premier filtrage peut être fin (cas des indicateurs de compromission de menaces cyber non classifiées) ou plus grossier (Range IP / BGP area / Domain Names, etc de zones d'intérêt).*
*Un **second filtrage** (**automatisé**) au moyen d'autres outils et équipements (qu'il n'y a pas lieu de décrire dans le cadre de cet arrêté royal qui détaille exclusivement le concours attendu des opérateurs et fournisseurs de Sv) aura lieu sur l'architecture classifiée du SGRS pour **uniquement** cibler le trafic des organisations et groupements repris dans les listes dont question à l'Art 44/3. **Ce second filtrage est classifié et extrêmement précis.***
*A **l'issue de ce second filtrage**, une période de traitement de 6 mois est prévue pour permettre aux agents du SGRS d'évaluer la pertinence des données collectées et pré-processées par les 2 étages de filtrage. Les données non pertinentes seront supprimées (par réécriture) alors que les données pertinentes seront stockées pour analyse ultérieure et rapportage.*

[…].

Par rapport aux autres questions posées :

1. […][44].
2. […][45].
3. *Finalement, les messages liés au routage, aux noms de domaine et aux autorités de certification peuvent faire l'objet d'une interception si le lien effectif est établi entre certains de ces messages et les listes prévues à l'Art 44/3* » (mise en gras et soulignement adaptés par l'Autorité).

56. Le Projet et les informations complémentaires communiquées par le demandeur appellent les commentaires suivants de la part de l'Autorité.

II.4.3. Analyse et position de l'Autorité

57. **Premièrement**, si l'Autorité comprend bien évidemment qu'un cadre normatif (loi ou arrêté royal) ne doive pas porter sur l'ensemble des détails techniques des **opérations de traitement de données**

[44] Ce passage cité au considérant n° 26.

[45] Voir la réponse citée au considérant n° 16.

envisagées, elle doit néanmoins pouvoir **comprendre concrètement celles-ci afin de pouvoir évaluer utilement si** le cadre normatif est adapté et si celles-ci et ce cadre respectent les règles de protection des données relevant de la compétence de l'Autorité. En l'occurrence, l'Autorité est bien consciente qu'elle n'est pas compétente pour contrôler les traitements de données mis en œuvre par les services de renseignements et de sécurité qui relèvent de la compétence du Comité permanent R. Cela étant précisé, l'Autorité est compétente à l'égard des traitements de données mis en œuvre par les opérateurs et fournisseurs de services de communications électroniques dans le cadre de leurs propres activités lorsqu'ils sont obligés de coopérer avec les services précités, comme elle l'a rappelé[46].

58. Dans ce contexte, l'Autorité est d'Avis qu'il convient également d'insister dans le présent Avis sur la **position suivante exprimée par le Comité R dans le considérant n° 11 de son propre Avis** :

> « ***Le citoyen*** *a* ***le droit de contrôler les activités des services de renseignement****.* ***Pour que ce contrôle soit*** **efficace***, certaines conditions préalables doivent être remplies. Ainsi, le Comité considère que tout système ou équipement utilisé par un service de renseignement pour le traitement automatisé de données (à caractère personnel)* ***doit satisfaire techniquement à l'exigence d'explicabilité*** *(mieux connue dans le jargon informatique sous le nom de principe* [d]'explainability*) et que cette possibilité technique doit être juridiquement établie.*
>
> *En ce qui concerne la réglementation soumise pour avis, le Comité estime que* ***cette obligation doit être explicitement incluse dans le Projet****, étant donné que la collecte d'informations au moyen d'un flux automatisé de (méta)données rend nécessaire de pouvoir expliquer, tant a priori qu'a posteriori, comment le système est parvenu à un résultat bien déterminé. Par ailleurs, la traçabilité n'est pas seulement importante pour le contrôle externe du fonctionnement et des résultats du système. Il est au moins aussi important que les agents du SGRS puissent vérifier ces éléments pour des raisons opérationnelles et à des fins de contrôle interne* » (mis en gras et souligné par l'Autorité, italiques enlevés pour être conformes à la mise en italiques dans le texte original).

59. **L'Autorité partage l'Avis du Comité R** : il convient d'adapter le Projet en ce sens.

60. **Deuxièmement**, **il est bien attendu des opérateurs et fournisseurs de services de communications électroniques qu'ils mettent en œuvre des traitements de données** à caractère personnel. Conformément au RGPD[47] (et pas seulement[48]) constitue un tel « traitement » : « *toute*

[46] Voir le considérant n° 41.

[47] Article 4, 2), du RGPD.

[48] Se référer à ce sujet aux autres règles de protection des données à caractère personnel.

opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ». Or, l'opérateur ou le fournisseur concerné doit placer (à supposer que cela soit un critère déterminant, *quod non*, le rôle de l'opérateur est de toute façon bien *actif* à cet égard) sur son infrastructure de réseau un (ou plusieurs) « *système(s) technique(s)* » (auquel le demandeur se réfère également via les termes « *solution technique* » ou « *mécanisme technique* ») qui permet de dupliquer des flux de données de communications électroniques « *vers* » des équipements du SGRS qui se trouveront « *chez* » ce prestataire de service.

61. **Troisièmement**, l'Autorité comprend que le système d'interception mis en place comporte les **trois phases de sélection/filtrage suivantes,** dont les deux dernières, dans la structure actuelle du Projet, ne relèvent pas de sa compétence :

- Tout d'abord, le **système technique** mis en place par l'opérateur ou le fournisseur de service de communications électroniques sur son infrastructure réseau, **sélectionne et duplique de manière automatisée** « *certains flux de données* » (**y compris les données de contenu** des communications), des « *communications électroniques émises ou reçues à l'étranger* », ou encore « *le trafic d'intérêt* » pour le SGRS, à destination d'équipements du SGRS (pour la réalisation d'un premier filtrage) ; ci-après, « **la sélection des flux de données** » ;

- Ensuite, un **premier filtrage automatisé et non classifié** est réalisé par le SGRS, via des équipements qui sont **placés chez l'opérateur ou le fournisseur** de service de communications électroniques concernés (« *soft filtering* ») ; ci-après, « **le premier filtrage** » ;

- Enfin, un **second filtrage – « extrêmement précis »** selon le demandeur **– automatisé et classifié** a lieu sur l'architecture classifiée du SGRS pour uniquement cibler le trafic des organisations et groupements repris dans les listes pertinentes (« *hard selection* ») ; ci-après, « **le second filtrage** ».

62. **Quatrièmement**, s'agissant de **la sélection des flux de données**, les critères de paramétrage du (ou des) « système(s) technique(s) » à mettre en place par l'opérateur (à un ou des endroits de son réseau à déterminer) à spécifiquement certains types de ces communications, s'agissant de trafic d'intérêt pour le SGRS, **sont indéterminés**. **Ni la Loi R&S, ni le Projet, ni les réponses communiquées par le demandeur ne permettent à l'Autorité d'identifier sur la base de quels critères concrets/techniques et dans quelles circonstances**, le « système technique » mis en place par

l'opérateur **sélectionnera les flux de données pertinents pour un filtrage subséquent par le SGRS, selon le type de service concerné**. En d'autres termes, l'Autorité n'est pas en mesure d'identifier **la capacité discriminante/filtrante/ciblante – et la mesure de cette capacité – des systèmes techniques** à mettre en place, à l'égard de l'ensemble des flux de données qui transitent sur l'infrastructure des prestataires de services concernés par le Projet.

63. Quoi qu'il en soit, juridiquement, **le dispositif du Projet ne peut pas prévoir que** « *Le fournisseur d'un service de communications électroniques ou l'opérateur du réseau met en place un système technique garantissant la transmission automatique des flux de données et de métadonnées de communications émises ou reçues à l'étranger* ». Tout d'abord, cette formulation **ne reflète pas les nuances – cependant insuffisantes – communiquées** par le demandeur. Ensuite, plus fondamentalement, une telle disposition est **contraire à l'arrêt de la Cour de Justice du 6 octobre 2020, Privacy International[49]**. En effet, elle laisse la porte ouverte à une **transmission généralisée et indifférenciée** de métadonnées de communications électroniques **et en outre en l'occurrence**, de **données de contenu**. La condition normative selon laquelle les communications concernées doivent être **émise ou reçue à l'étranger** (**y compris** l'hypothèse où la communication est **émise et reçue à l'étranger**), **à supposer qu'elle puisse être effectivement mise en œuvre** (**ce que le demandeur ne démontre pas**, notamment compte-tenu du type de service concerné), est **excessivement générale et susceptible d'autoriser l'interception disproportionnée** de quantités très importantes de communications électroniques sans le moindre lien avec les missions du SGRS. Par exemple, peuvent être visées de manière indiscriminée toutes les communications émises depuis un pays A, reçues dans un pays A et émises et reçues dans ce pays A, transitant via les services concernés. **L'Autorité rejoint sur ce point la conclusion défavorable de la CPVP en 2016, au considérant n° 37 de son Avis[50]**. Elle souhaite encore mettre en avant le passage suivant du **rapport communiqué par l'Expert désigné par l'Autorité, qu'elle rejoint également** :

> « *De gekozen strategie, waarbij potentieel zeer omvangrijke communicatiestromen bij de operatoren worden gedupliceerd en vervolgens in twee stappen gefilterd,* ***brengt een ernstig risico mee op informatievergaring op grote schaal of "mass surveillance".*** *Het voorbeeld dat gegeven worden in de toelichting is het afluisteren van de communicatie van de intelligentiedienst van Redland is inderdaad zeer redelijk, maar het is even goed mogelijk dat het gaat om de communicatie van een volledig land of zelfs een volledig continent.* ***Het feit dat de twee stappen van filtering onder volledige controle van ADIV gebeuren, betekent dat het niet kan uitgesloten worden dat gegevens op grote schaal verwerkt worden,*** *in een systeem vergelijkbaar met XKeyscore (NSA) of*

[49] Aff. C-623/17.

[50] Voir le considérant n° 9.

Tempora (GCHQ) zoals beschreven in de documenten gelekt door Snowden. Ook bestaat er het risico dat deze gegevens worden gedeeld met derde landen » (mis en gras par l'Autorité).

64. *A priori*, **il semblerait en tout cas, que le premier filtrage** (non classifié) **doive être réalisé par l'opérateur ou le fournisseur de service de communications électronique lui-même,** et non par le SGRS. **Et le cadre normatif applicable, en principe la Loi R&S, devrait le prévoir**. Notamment, il conviendrait de fixer dans ce contexte, **la granularité/l'étendue** des **« zones géographiques »** potentiellement concernées. **L'Autorité réserve néanmoins son analyse à ce sujet** (à défaut pour celle-ci de disposer de suffisamment d'informations en la matière).

65. Le cadre normatif applicable doit prévoir de **communiquer aux opérateurs et fournisseurs de services de communications électroniques des critères conformes à la jurisprudence de la Cour de Justice** en matière de dérogations à la confidentialité des communications électroniques, **sur la base desquels ils sélectionneront, via leurs systèmes, les communications électroniques à intercepter et transmettre** vers les équipements du SGRS, **dans les limites de ce qui est nécessaire** à ce dernier, pour l'exercice de ses missions. Et comme l'Autorité l'a déjà souligné, « *la nécessité de traiter des données sera in concreto* ***appréciée compte-tenu de la finalité du traitement*** *et de la phase d'exercice de la mission concernée (la nécessité d'une donnée pourra varier selon le cycle du renseignement ; notamment, ce n'est pas parce qu'une donnée ne s'avère plus nécessaire dans une phase ultérieure d'exercice de la mission concernée, qu'elle ne l'était pas dans sa phase initiale)* » (mis en gras par l'Autorité dans le présent Avis)[51].

66. Dans ce contexte, **l'Autorité doute qu'il soit possible de manière générale dans une seule disposition, de régler toutes les hypothèses envisagées, abstraction faite du type de service concerné** (Service de communications (couche de liaison de données) - Service d'accès à internet (IP), Service MPLS Multiprotocol Label Switching, Services de téléphonie (3G-4G-4G), Services de communication par satellite, Services de VPN/proxy/Tor/mixnet ; Service de messagerie e-mail sans chiffrement de bout en bout (type Gmail) ; Service de messagerie e-mail avec chiffrement de bout en bout (type Proton) ; Service de messagerie instantanée type Signal (conservation minimisée de métadonnées) ; Service de messagerie instantanée type WhatsApp (conservation plus large de métadonnées) ; Services de réseau social). En tout état de cause, **chaque type de service concerné nécessite une réflexion appropriée**. L'Autorité semble comprendre que le Projet a principalement été pensé à l'égard des opérateurs.

[51] Et comme l'Autorité l'a déjà souligné, « *la nécessité de traiter des données sera in concreto* ***appréciée compte-tenu de la finalité du traitement*** *et de la phase d'exercice de la mission concernée (la nécessité d'une donnée pourra varier selon le cycle du renseignement ; notamment, ce n'est pas parce qu'une donnée ne s'avère plus nécessaire dans une phase ultérieure d'exercice de la mission concernée, qu'elle ne l'était pas dans sa phase initiale)* » (mis en gras par l'Autorité dans le présent Avis), Avis n° 34/2024 du 15 avril 2024 concernant une Proposition de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour (CO-A-2024-139), considérant n° 28.

67. **Cinquièmement,** compte-tenu des missions du SGRS, l'Autorité comprend **l'objectif de minimiser l'échange d'informations** avec les opérateurs et fournisseurs de services de communications électroniques. Cependant, l'Autorité a déjà mis en évidence[52] que **la sollicitation de la collaboration** de fournisseurs de services de communications électroniques dans le cadre du traitement de données à caractère personnel **implique par définition un échange d'informations** avec ceux-ci. En tant que responsables du traitement, ils sont également tenus de veiller à la licéité des traitements de données qu'ils mettent en œuvre en vertu de l'obligation légale qui leur incombe.

68. Or **le droit belge met en place des garanties spécifiques prenant en compte la sensibilité de la coopération mise en œuvre** avec les services de renseignement et de sécurité (notamment), à savoir en particulier : les articles 36 et 37 de la **Loi R&S** prévoient une obligation de secret ; l'article 127/3 de la **Loi du 13 juin 2005** ***relative aux communications électroniques*** prévoit la constitution auprès de chaque opérateur d'une Cellule de coordination chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques (voir spécialement son paragraphe 2) ; les articles 11, 12 et 13 de la **LTD elle-même** consacrent une série de dérogations aux droits des personnes concernées s'agissant des données traitées par des entités qui d'une manière ou d'une autre, interagissent avec les services de renseignements et de sécurité, tandis que l'article 92 de la LTD allège d'autres obligations de ces entités ; et enfin, la **Loi du 11 décembre 1998** ***relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé*** organise la protection des informations classifiées.

69. En conclusion, l'Autorité est d'avis que le Projet doit être significativement adapté. Plus fondamentalement, ce sont les articles 44 et 44/5 de la Loi R&S eux-mêmes qui devraient être clarifiés en la matière. **La coopération des opérateurs de réseau et des fournisseurs de services de communications électroniques dans le cadre des articles 44 et 44/5 de la Loi R&S et du Projet devrait faire l'objet un débat parlementaire actualisé** et être encadrée par des dispositions normatives dépourvues d'ambiguïté.

70. Ces constatations sont bien évidemment sans préjudice des possibilités de traitements de données que le SGRS peut lui-même mettre en œuvre, à l'étranger ou en Belgique, sous sa responsabilité exclusive (c'est-à-dire, sans la coopération des opérateurs et fournisseurs concernés), conformément à la Loi R&S, traitements qui pour rappel, ne relèvent pas de la compétence de l'Autorité mais bien de celle du Comité R.

---

[52] Voir Autorisation (délivrée) n° 001/2025 du 18 juillet 2025 *concernant une demande d'autorisation visée à l'article 21, § 4, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique : « Command-and-Control servers communicatiemetadata – waarschuwing » (AH-2025-0034)*, considérant n° 89.

PAR CES MOTIFS,
L'Autorité est d'avis que :

1. Il convient de se référer à titre préliminaire à l'Avis de la CPVP de 2016 à propos du projet qui est devenu la Loi de 2017, et à la position défavorable de la CPVP à propos de l'article 44/5 de la Loi R&S (**considérants nos 8-9**) ;

2. Dans la lignée de la position exprimée par le Conseil d'Etat et compte-tenu de l'ingérence causée par les articles 44 et 44/5 de la Loi R&S, la mise en œuvre de ces dispositions et de la coopération des opérateurs et fournisseurs de services de communications électroniques, les missions du SGRS doivent être interprétées de manière prudente et dans le strict respect des principes de subsidiarité et de proportionnalité (**considérants nos 10-12**) ;

3. Le dispositif du Projet doit être adapté et clarifier que ne sont permises que les interceptions de communications électroniques transitant via les services accessibles en Belgique de l'opérateur ou du fournisseur concerné. Il doit indiquer qu'il est limité à la collaboration avec les opérateurs et fournisseurs de services de communications électroniques qui offrent leur service en Belgique et recourent à cette fin à une infrastructure technique pertinente au regard du service ou réseau concerné, sur le territoire belge et sur laquelle il exerce un contrôle suffisant compte-tenu de la coopération envisagée. Quant aux types de services concernés, la coopération prévue a pour objectif de s'appliquer largement à quiconque fournit un service consistant à offrir à ses clients une possibilité d'échange électronique d'informations (**considérants nos 13-17**) ;

4. Le dispositif du Projet ne prévoit pas d'obligation de coopération des opérateurs et fournisseurs de communications électroniques au déchiffrement des communications électroniques *in fine* concernées par les interceptions. Si l'auteur du Projet a l'intention de prévoir cette coopération, il lui incombe d'adapter le dispositif du Projet, en prenant en considération les développements du présent Avis. Il conviendra de prévoir explicitement dans le dispositif du Projet à tout le moins : que premièrement, la coopération au déchiffrement des communications électroniques concernées ne concerne que la solution technique de chiffrement mise en œuvre par l'opérateur ou le fournisseur de service de communications électronique sollicité lui-même ; que deuxièmement, cette coopération ne peut pas avoir pour effet de diminuer la qualité de la solution technique de chiffrement choisie par cet opérateur ou fournisseur, pour les autres utilisateurs dont les communications électroniques ne doivent pas être interceptées ; et que troisièmement, le concours de l'opérateur ou du fournisseur ne peut pas être demandé pour déchiffrer des communications chiffrées de bout en bout ou au

niveau applicatif. Ce sujet devrait être l'objet d'un débat parlementaire actualisé (**considérations nos 18-29**) ;

5. Il appartient au Conseil d'Etat de se prononcer quant à la conformité du Projet au regard du droit international public, et selon ses conclusions, il incombe à l'auteur du Projet d'en tirer les conséquences sur le plan de la licéité des traitements de données envisagés (**considérants nos 30-31**) ;

6. Sur la base des informations communiquées et disponibles, l'Autorité n'est pas en mesure de se prononcer quant à la question de savoir si les articles 44 et 44/5 de la Loi R&S doivent bénéficier d'un régime de contrôle préalable *ad hoc* moins contraignant que le contrôle applicable aux méthodes exceptionnelles de recueil de données. Il convient sur ce point, de consulter le Comité R et d'en tirer les conséquences sur le plan de la licéité des traitements envisagés. En tout état de cause, la motivation du cadre légal actuel doit impérativement être étayée (**considérants nos 32-39**) ;

7. Compte-tenu de l'ingérence importante causée par les articles 44 et 44/5 de la Loi R&S dans les droits et libertés des personnes concernées, l'Autorité ne voit pas sur quelle base, à l'aune de la jurisprudence européenne en matière de dérogations à la confidentialité des communications électroniques, il serait justifiable de dispenser le SGRS d'une décision (autorisation) préalable de la Commission BIM (ou du Comité Permanent R), sauf cas d'urgence, à la manière dont est encadré en droit positif le recours aux méthodes exceptionnelles de recueil de données. Il convient de garantir au Comité R le temps et les moyens financiers, techniques et humains nécessaires afin de réaliser le contrôle organisé par le Projet (**considérants nos 41-47**) ;

8. Le Projet doit mettre en œuvre l'exigence d'explicabilité technique conformément au considérant n° 11 de l'Avis du Comité R et l'Autorité doit pouvoir être en situation de comprendre les opérations de traitement envisagées (**considérants nos 58-59**).

9. En l'état, le dispositif du Projet est disproportionné en ce qu'il peut permettre la sélection et redirection disproportionnées de flux de donnés sans relation avec les missions du SGRS, vers les équipements de celui-ci. Le cadre normatif applicable doit prévoir de communiquer aux opérateurs et fournisseurs de services de communications électroniques des critères conformes à la jurisprudence de la Cour de Justice en matière de dérogations à la confidentialité des communications électroniques, sur la base desquels ces prestataires de services sélectionneront via leurs systèmes, les communications électroniques à intercepter et les transmettront vers les équipements du SGRS, dans les limites de ce qui est nécessaire à

ce dernier, pour l'exercice de ses missions. Il est nécessaire de mener en la matière une réflexion appropriée pour chaque type de service concerné (**considérants nos 56-69**).

Ces constatations sont bien évidemment sans préjudice des possibilités de traitements de données que le SGRS peut lui-même mettre en œuvre, à l'étranger ou en Belgique, sous sa responsabilité exclusive (c'est-à-dire, sans la coopération des opérateurs et fournisseurs concernés), conformément à la Loi R&S, traitements qui pour rappel, ne relèvent pas de la compétence de l'Autorité mais bien de celle du Comité R (**considérant n°70**).

10. A l'aune de ces éléments et des développements du présent avis, il est recommandé que la coopération des opérateurs de réseau et des fournisseurs de services de communications électroniques dans le cadre des articles 44 et 44/5 de la Loi R&S et du Projet fassent l'objet un débat parlementaire actualisé, et soit encadrée par des dispositions normatives dépourvues d'ambiguïté (**considérants nos 29-69**).

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice