AVIS 2026/007 DU 3 JUIN 2026

PROJET DE LOI MODIFIANT LA LOI RENSEIGNEMENT ET LA LOI CLASSIFICATION

Vu le courrier du 29 avril 2026 de la ministre de la Justice au Comité R/I, transmis par e-mail le 30 avril 2026, par lequel une demande d'avis a été introduite concernant l'avant-projet de loi « modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 16 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé » (ci-après : le projet de loi).

Compétence du Comité R/I

Vu l'article 33, alinéa 8, de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace ;

Vu les articles 73, 95, 107 et 128 de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Normes juridiques à modifier et propositions du Comité

Le projet de loi vise à modifier et à ajouter diverses dispositions de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après : la Loi Renseignement ; en abrégé : L.R&S). Le projet de loi vise à également à compléter l'article 16 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé (ci-après : la Loi Classification ; en abrégé : L.C&HS).

Outre une évaluation générale et une analyse juridique et technique ainsi qu'une évaluation législative des dispositions légales proposées, qui suit l'ordre du projet de loi, le présent avis contient des propositions concrètes (**REC-1 à REC-79 inclus**).

AVIS

ÉVALUATION GÉNÉRALE

1. Le Comité **reconnaît la nécessité d'un État résilient, capable de faire face à des menaces** telles que l'espionnage, l'ingérence, l'extrémisme et le terrorisme. C'est la raison pour laquelle le Comité est en principe favorable aux modifications législatives qui confèrent de nouvelles compétences à la VSSE et au SGRS, comme par exemple la décision d'accorder désormais aux services de renseignement certains pouvoirs d'action, alors que leur rôle en la matière restait auparavant « limité », au sein de la chaîne de sécurité, à la collecte et à l'analyse de renseignements ainsi qu'à la mise à disposition d'autres autorités afin que celles-ci puissent, le

cas échéant, prendre les mesures appropriées. Même s'il s'agit là d'un véritable changement de paradigme, le Comité estime que mélanger les services de renseignement et les services d'action peut constituer un choix légitime, mais que, **d'une part, la nécessité opérationnelle doit être démontrée plus clairement dans l'exposé des motifs**, et, **d'autre part, qu'il est également crucial, dans l'intérêt du maintien de l'ordre juridique démocratique, de renforcer le contrôle démocratique sur les services de renseignement**. Ce contrôle renforcé constituera, d'une part, une garantie pour la protection de la société et des droits des citoyens individuels et, d'autre part, préservera les services eux-mêmes de toute suspicion injustifiée. Cette remarque vaut d'ailleurs aussi pour d'autres compétences nouvelles et étendues qui figurent dans le projet et qui, combinées aux possibilités déjà existantes, permettent à ces services d'agir de manière très ciblée et énergique. Mais le revers de la médaille est naturellement que des garanties solides doivent être prévues contre d'éventuels abus.

Le Comité rappelle à cet égard que l'**accord de gouvernement fédéral** exprimait également la volonté de renforcer **le contrôle démocratique sur les services de renseignement** (accord de gouvernement fédéral 2025-2029, p. 142). Bien que l'exposé des motifs fasse référence à plusieurs reprises au contrôle exercé par les organes compétents afin de garantir les droits fondamentaux, le Comité constate que cette intention n'apparaît pas suffisamment dans le présent avant-projet. Le Comité doit au contraire constater que, face à l'extension (légitime) des compétences des services de renseignement, une attention insuffisante a été accordée à la qualité de la nouvelle réglementation et à un contrôle approprié, efficace et effectif par le Comité ou la Commission BIM, et que même les garanties existantes sont réduites ou supprimées. Le Comité ne peut pas être d'accord. L'équilibre nécessaire entre, d'une part, des compétences étendues pour les services publics opérant dans un État de droit et, d'autre part, le contrôle démocratique de celles-ci, comme il sied à un État de droit, ainsi que l'ambition affichée par le gouvernement fédéral de renforcer le contrôle démocratique sur les services de renseignement, exigent, à l'estime le Comité, que **les remarques suivantes** soient intégrées dans le présent projet.

(1) CYBER

2. L'exposé des motifs indique ce qui suit : *« Les technologies utilisées aujourd'hui par les cybers acteurs malveillants nécessitent de disposer d'outils proactifs qui vont accorder au Service Général du Renseignement et de la Sécurité (SGRS) et à la Sûreté de l'Etat (VSSE) le pouvoir de répondre efficacement aux menaces issues du cyberespace. »*.[1] Et ensuite : *« Compte tenu des cyberattaques de plus en plus fréquentes auxquelles s'exposent de manière générale les services publics belges et, particulièrement, les services sensibles tels que les services de renseignement et de sécurité, il est important de disposer d'un cadre juridique qui offre la possibilité à ces services d'assurer au mieux leurs missions. »*.[2]

Le Comité reconnaît la nécessité de disposer d'un cadre juridique suffisamment solide pour les services de renseignement dans le contexte de la lutte contre les menaces dans le cyberespace. Les remarques ci-dessous portent uniquement sur les implications juridiques de cette question.

Notion de moyen technique : reconnaissance technique et recherche proactive dans le cyberespace (projet d'article 3, 14 L.R&S)

3. Le Comité estime que l'ajout, pour le SGRS (et la VSSE)[3], d'une compétence permettant de mener une « reconnaissance technique » et une « recherche proactive » technique est justifié.

---

1 Exposé des motifs, p. 2.
2 Exposé des motifs, p. 17.
3 D'après l'exposé des motifs, cette modification semble surtout servir les intérêts du SGRS, en particulier le Commandement cyber qui en fait partie.

Le projet de loi ajoute deux exceptions à la définition de « moyen technique » à l'article 3, 14° L.R&S :
« c) des configurations ou dispositifs utilisés pour chercher et analyser l'état technique, les caractéristiques ou la configuration des systèmes informatiques et de communications et ce, dans des lieux accessibles au public dans le cyberespace » – c'est-à-dire : les outils permettant une recherche proactive dans le cyberespace ;
« d) des configurations ou dispositifs utilisés à des fins de reconnaissance préalable, de repérage fonctionnel, ou d'analyse de vulnérabilités et ce, dans des lieux accessibles au public dans le cyberespace » – c'est-à-dire : les outils permettant une reconnaissance technique dans le cyberespace.

La recherche proactive vise à *« obtenir un état technique de l'exposition des systèmes (protocoles utilisés, ports ouverts, certificats SSL/TLS, etc.). Cette dernière s'apparente à un relevé topographique numérique ou à un inventaire fonctionnel d'une zone réseau. Cette recherche permet alors de rechercher, d'identifier et de valider les empreintes techniques des acteurs malveillants[4] »*.[5]
« Plus particulièrement », la reconnaissance technique *« consiste, par exemple, à recenser les caractéristiques techniques d'une l'infrastructure informatique accessibles via Internet, à identifier les services techniques actifs (tels que les interfaces de gestion, les serveurs de messagerie ou les bases de données publiquement accessibles), l'enregistrement des versions logicielles indiquées ou déductibles et la détection de toute configuration susceptible de présenter une vulnérabilité connue dans la littérature spécialisée et des traces d'une éventuelle utilisation abusive par des acteurs malveillants. »*.[6]

L'exposé des motifs précise, en outre, que ces deux actes d'enquête **relèvent actuellement de l'article 18/4, § 1er L.R&S** (en particulier une observation à l'aide de moyens techniques depuis des lieux accessibles au public).[7] L'exposé des motifs donne ensuite une description détaillée du fonctionnement concret des actes concernés et explique pourquoi la procédure d'autorisation des méthodes spécifiques dans ce cadre est *de facto* inefficace. Cette explication convainc le Comité de la nécessité de créer un cadre juridique pour ces deux actes, ainsi que le caractère non approprié à cet effet de la procédure relative aux méthodes spécifiques.

Néanmoins, **le Comité n'approuve pas la manière dont cela est mis en œuvre sur le plan juridique**. Le Comité constate effectivement que le projet de loi ne crée pas de véritable fondement juridique pour les pouvoirs d'enquête en question. D'un point de vue technico-juridique, seules deux exceptions supplémentaires sont ajoutées à la notion de moyen technique. Cette notion est utilisée dans la Loi Renseignement comme critère pour préciser l'application de certaines méthodes spécifiques de renseignement (en particulier les articles 18/4, 18/5 et 18/7 L.R&S). L'article 3, 14° ne peut en soi jamais constituer une base juridique justifiant un pouvoir d'enquête.

L'exposé des motifs établit lui-même un parallèle avec l'analyse proactive et non intrusive des systèmes de réseaux et d'information accessibles au public, qui permet au **Centre pour la Cybersécurité Belgique (CCB)** de détecter les systèmes de réseaux et d'information vulnérables ou mal configurés, en vertu de l'article 19, 9° 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.[8] Toutefois, dans cette disposition légale également, les actes d'enquête concernés sont décrits comme une compétence du CCB, et non comme une exception à un moyen technique.

4 Passage souligné par le Comité.
5 Exposé des motifs, p. 18.
6 Exposé des motifs, p. 19.
7 *Ibid.*
8 Exposé des motifs, p. 20.

Cette approche ne fournit donc pas de base juridique suffisante pour les deux pouvoirs d'enquête mentionnés, mais se contente tout au plus de préciser ce qui ne relève plus d'un pouvoir d'enquête existant (en particulier l'article 18/4, § 1er L.R&S). Compte tenu de cette approche adoptée dans le projet de loi, une reconnaissance technique et une recherche proactive dans le cyberespace ne reposent plus sur une base juridique spécifique, mais uniquement sur la règle permissive (à savoir que tout ce qui n'est pas explicitement interdit est autorisé). Au regard de l'article 8 CEDH et de l'article 22 de la Constitution, les actes d'enquête en question vont cependant trop loin pour se fonder uniquement sur la règle de permissivité. Afin de créer une base juridique solide pour les pouvoirs d'enquête concernés, **ces derniers doivent être réglés par un article de loi distinct**, comprenant une énumération claire des conditions applicables et des mécanismes de contrôle correspondants.

La méthode consistant à prévoir des exceptions à la notion de moyen technique permettra également de **soustraire entièrement** les actes concernés **au contrôle de la Commission BIM, ce qui, à l'estime du Comité, n'est pas justifié.**

Pour toutes les raisons susmentionnées, **le Comité considère que l'utilisation de configurations ou d'appareils dans le cadre de la recherche proactive susmentionnée ou de la reconnaissance technique susmentionnée doit faire l'objet d'une disposition législative distincte. Le Comité R/I recommande d'accorder à cet égard un pouvoir de contrôle correctif (REC-1) au Comité (comme contrôleur de deuxième ligne) mais aussi à la Commission BIM (comme contrôleur de première ligne).**

Intrusion informatique (projet d'article 44/6 L.R&S)

4. L'exposé des motifs indique que *« [l']article 44/1 autorise le SGRS à procéder à des intrusions dans des systèmes informatiques situés à l'étranger dans le cadre de certaines de ses missions. Toutefois, la rédaction actuelle ne précise pas si ces intrusions peuvent s'effectuer via des intermédiaires tels que des logiciels, services ou hébergeurs tiers reliés aux systèmes visés. Or, dans la pratique, les systèmes informatiques visés s'appuient presque systématiquement sur des infrastructures externes gérées par des entités tierces. Cette situation crée une incertitude juridique quant à la possibilité d'accéder à un système par l'intermédiaire d'un outil tiers alors que le système informatique concerné est bien un système lié à une organisation ou institution visées à l'article 44/3.*
En effet, les entités ciblées ne disposent plus nécessairement de serveurs ou d'infrastructures informatiques internes. Dans la très grande majorité des cas, leurs systèmes sont hébergés sur des plateformes externes, appuyés sur des outils tiers (tels que des services de messagerie ou des services de sécurité informatique) ou gérés par des sous-traitants techniques. Dans ce contexte, une intrusion réellement efficace ne peut souvent être réalisée qu'en passant par ces intermédiaires techniques, qui servent d'accès indirect au système final. Par exemple : si la cible fait appel à un prestataire informatique pour la gestion de son réseau, ce prestataire constitue un point d'entrée potentiel pour accéder au système.
En l'absence de cette précision, le libellé de l'article 44/1 ne permet pas de couvrir explicitement la situation susvisée, de telle sorte qu'il subsiste une insécurité juridique à cet égard. Il est important de noter que le fait de passer via un vecteur tiers n'engendre aucun dommage pour celui-ci et que, dans la plupart des cas, ce procédé est l'unique moyen d'accéder au système visé. Il faut aussi souligner que le vecteur tiers n'est pas la cible du SGRS mais constitue un moyen d'accéder au système final appartenant à une institution ou organisation des listes de l'article 44/3. Enfin, cette possibilité reste pleinement encadrée non seulement via les contrôles mentionnés à l'article 44/3, mais également via l'inclusion d'un contrôle spécifique en la matière dans cette même disposition. Cela permettra au Comité R d'avoir une vue sur les outils externes effectivement utilisés par le SGRS et ce, dans le cadre de son contrôle postérieur visé dans l'article précité. ».[9]

[9] Exposé des motifs, p. 81-82.

Le projet d'article 44/6, § 1er L.R&S prévoit ce qui suit :
« *[l']intrusion prévue à l'article 44/1* » – on entend par là l'intrusion dans un système informatique situé à l'étranger – « *peut être mise en œuvre à l'aide de logiciels, de services ou d'hébergeurs tiers utilisés par le système informatique concerné ou qui y sont liés. Une telle intrusion ne peut être effectuée que pour des motifs techniques, nécessaires soit pour assurer l'exécution optimale de la mission, soit pour garantir la sécurité de celle-ci ou de l'agent.* ».

5. Le Comité estime que, dans le cadre de l'application de la réglementation susmentionnée, **il doit exister un système de reporting interne à ce sujet, qui doit être prescrit par la loi et tenu à la disposition du Comité à tout moment lors de son contrôle spécifique prévu pour cette méthode particulière de renseignement (REC-2).**

6. Le Comité **n'a retrouvé, dans l'exposé des motifs, aucune justification de la nécessité d'une telle intrusion** « *pour garantir la sécurité de l'agent* ».[10] **Le Comité recommande soit d'expliquer cette justification dans l'exposé des motifs, soit de supprimer le passage concerné de la disposition législative (REC-3).**

7. Initialement le système d'interception prévu aux articles 44 et suivants L.R&S prévoyait des interceptions ciblées et non massives. Le contrôle du Comité R/I est supposé suffire pour garantir le caractère ciblé et non généralisé.[11]
Cependant, comme l'a relevé récemment l'APD dans un de ses avis sur un projet d'arrêté d'exécution de la L.R&S : « *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.* »[12]
Dans ces conditions, **le Comité invite le législateur à revoir le régime des interceptions repris aux articles 44 et suivants, en tenant compte notamment de la jurisprudence récente de la Cour de justice de l'UE et de la CEDH (en particulier l'arrêt dans l'affaire Centrum för Rättvisa c. Suède (Requête n°35252/08) (REC-4).**

(2) OBLIGATION DE COMMUNICATION D'INFORMATIONS PAR LES PERSONNES ET LES ORGANISATIONS QUI REMPLISSENT UN SERVICE D'INTÉRÊT PUBLIC

8. Le projet de loi vise à préciser le droit de réquisition de la VSSE et du SGRS vis-à-vis des services publics (article 14 L.R&S).[13] L'exposé des motifs indique ce qui suit : « *Dans le cadre de la collaboration avec les services de renseignement et de sécurité, une précision est apportée au sujet des institutions qui remplissent un service d'intérêt public général. A l'heure actuelle, les tâches ou services d'intérêt public ne sont plus exclusivement accomplies par des autorités publiques. Il est de plus en plus courant que l'exécution de ces tâches d'intérêt public*

10 Passage souligné par le Comité.
11 « *Le ministre de la Défense remarque que la règle de la proportionnalité s'applique et que le Comité R ne manquerait pas d'intervenir si le SGRS devait pratiquer des écoutes généralisées. Le Comité R préviendra le Parlement et demandera l'interruption immédiate d'écoutes qui ne sont pas ciblées.* » (*Doc. parl.*, Sénat, 2002-2003, Rapport, 2-1412/3, p. 10).
12 Avis APD 118/2025, n° 63.
13 Exposé des motifs, p. 27.

soient transférées vers des organisations privées ou hybrides. Pour rencontrer cette réalité, plusieurs dispositions de la loi sont adaptées (articles 3, 29°,14,16 et 18/6/1). » .[14]

Concrètement, l'article 3 29° ajoute et décrit la notion d' « autres personnes et organisations qui remplissent un service d'intérêt public ». Des modifications sont apportées au pouvoir de requérir des informations auprès des services publics (art. 14 L.R&S), de requérir des informations auprès des personnes et des organisations du secteur privé (art. 16 L.R&S) et de requérir des données de transport et de voyage auprès de tout fournisseur privé de service en matière de transport ou de voyage (art. 18/6/1 L.R&S).

L'article 14, alinéa 2 L.R&S est modifié comme suit (le soulignement a été ajouté) :
« A la requête d'un service de renseignement et de sécurité, les autorités judiciaires les fonctionnaires et les agents des services publics, y compris des services de police, et toutes les autres personnes et organisations qui remplissent un service d'intérêt public général pour la partie de leurs activités qui relèvent de ce service d'intérêt public général, communiquent au service de renseignement et de sécurité concerné les informations utiles à l'exécution de ses missions. ».

Le projet d'**article 3, 29° L.R&S** définit la notion des « autres personnes et organisations qui remplissent un service d'intérêt public général » comme suit :
« a) les personnes, quelles que soient leur forme et leur nature, qui :
i) ont été créés pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial, et ;
ii) sont dotés d'une personnalité juridique, et ;
iii) dépendent de l'Etat, des Régions, des Communautés, des autorités locales ou d'autres organismes publics ou de droit public, de l'une des manières suivantes :
1. soit leurs activités garantissant les intérêts essentiels de l'Etat ou les besoins essentiels de la population sont financées majoritairement par l'Etat, les Régions, les Communautés, les autorités locales ou d'autres organismes publics ou de droit public ;
2. soit leur gestion est soumise à un contrôle de l'Etat, des Régions, des Communautés, des autorités locales ou d'autres organismes publics ou de droit public ;
3. soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par l'Etat, les Régions, les Communautés, les autorités locales ou d'autres organismes publics ou de droit public ;
3 soit plus de la moitié des membres de l'organe d'administration, de direction
ou de surveillance sont désignés par l'Etat, les Régions, les Communautés, les autorités locales ou d'autres organismes publics ou de droit public ;
b) les associations formées par l'Etat, des Régions, des Communautés, des autorités locales ou d'autres organismes publics ou de droit public ou par une ou plusieurs personnes visées au point a) ; ».

À **l'article 16 L.R&S**, les mots *« et pour autant qu'elles ne relèvent pas du champ d'application de l'article 14 »* sont ajoutés. Cette modification **rend obligatoire**, dans une large mesure, la communication d'informations par toutes les entreprises et organisations privées qui remplissent des services d'intérêt général. En effet, cela signifie que ces acteurs, en ce qui concerne les données traitées dans le cadre de leur mission de service public, ne relèvent plus du champ d'application de l'article 16 L.R&S (communication facultative), mais dans celui de l'article 14 L.R&S (communication obligatoire). À titre d'illustration des types d'entités relevant de la notion de « personnes et organisations qui remplissent un service d'intérêt général », l'exposé des motifs renvoie aux annexes de la Loi du 26 avril 2024 relative à la cybersécurité, dans laquelle sont répertoriées diverses entreprises dans des secteurs critiques.[15] Toutefois, sur la base de la définition légale proposée, le champ d'application est beaucoup plus large. Les entreprises privées qui, en vertu des modifications prévues, seront tenues de fournir

[14] Exposé des motifs, p. 11.
[15] Exposé des motifs, p. 27.

des informations à la VSSE et au SGRS sont, par exemple : les université et les écoles (enseignement)[16], les autorités portuaires, les études de notaires, les études d'huissiers de justice, les sociétés de logement social, les entreprises d'énergie (gestion des réseaux), les sociétés de transport public certains établissements de soins, les mutuelles (par exemple dans le cadre de la gestion des allocations de chômage). **Cette obligation de communication s'accompagne de l'absence de contrôle préalable, indépendant et correctif (par exemple de la Commission BIM).**

À **l'article 18/6/1 L.R&S**, les mots *« à l'exception de ceux qui tombent sous l'application de l'article 14 »* sont ajoutés. **Le Comité constate que cela a pour conséquence que la collecte d'une multitude d'informations par la VSSE et le SGRS n'est plus soumise au contrôle BIM indépendant et correctif exercé par la Commission BIM et le Comité R/I (notamment la collecte la collecte de données relatives au transport et aux voyages dans les aéroports).** L'ajout des mots susmentionnés à l'article 18/6/1 fait de cette méthode spécifique *de facto* une méthode ordinaire (art. 14 L.R&S). Le Comité rappelle que si ces mêmes informations sont demandées par l'intermédiaire de l'Unité d'Information des Passagers, l'accord préalable de la Commission BIM est requis (art. 16/3 L.R&S), comme l'a prévu le législateur à la suite de l'arrêt de la Cour constitutionnelle relatif au PNR.[17]
Dans l'exposé des motifs, il est indiqué que *« les méthodes existantes de collecte de données prévues dans la loi organique sont modifiées sur plusieurs points. ».* Et il est ajouté que *« la protection des droits fondamentaux est garantie »*.[18] Au vu, ne serait-ce que des modifications apportées à l'article 18/6/1 L.R&S, le Comité ne peut souscrire à cette affirmation.

La notion « d'autres personnes et organisations qui remplissent un service d'intérêt public général » (projet d'art. 3, 29° juncto art. 14 L.R&S)

9. L'importance du pouvoir de réquisition des services de renseignement (art. 14 L.R&S) est reconnue depuis longtemps. Ainsi, l'exposé des motifs de la Loi BIM du 4 février 2010 indiquait déjà que *« [c]ompte tenu de la mission dévolue aux services de renseignement et de sécurité, qui consiste, entre autres, à protéger les intérêts fondamentaux de l'État, il est indispensable que tous les services publics apportent leur collaboration aux services de renseignement lorsqu'ils en font la demande. »*.[19] Concernant la portée de cette notion de « services publics », l'exposé des motifs de la Loi Renseignement du 30 novembre 1998 indique ce qui suit : *« La notion de service public doit être comprise dans son sens le plus large et comprend notamment tout organisme d'intérêt public (…) »*.[20]
Il convient de noter, à propos de cette dernière référence, qu'en 1998, la communication d'informations par les services publics était encore facultative et qu'elle n'est devenue obligatoire qu'en 2010.

10. Ni en 1998 ni en 2010, il n'y a eu de débat sur la portée exacte de la notion de « services publics ». Or, un tel débat s'impose en ce qui concerne les services publics dans leur dimension fonctionnelle. Le Comité constate que le projet de loi vise à clarifier le champ d'application personnel du droit de réquisition à l'égard des services publics (art. 14 L.R&S), en ajoutant et en définissant la notion d'« autres personnes et organisations qui remplissent un service d'intérêt public général ». L'exposé des motifs indique à cet égard ce qui suit : *« Les auteurs du projet se sont inspirés pour cette définition à la fois du champ d'application de la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité et du champ d'application de la loi du 26 avril 2024 établissant un cadre pour la*

16 Également mentionné dans l'exposé des motifs, p. 44.
17 Cour constitutionnelle, arrêt n° 131/2023 du 12 octobre 2023.
18 Exposé des motifs, p. 10.
19 *Doc. parl.* Sénat 2008-2009, n° 4-1053/1, p. 39.
20 *Doc. parl.* Chambre 1995-1996, n° 49-638/001, p.14.

cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. ».[21] Le Comité souligne tout d'abord que divers autres textes législatifs contiennent plus ou moins la même disposition, notamment, mais sans s'y limiter, la Loi du 30 juin 2018 relative à la protection de la vie privée (art. 5), la Loi du 17 juin 2016 relative aux marchés publics (art. 2, 1°) et la Loi du 4 mai 2016 relative aux données ouvertes et à la réutilisation des informations du secteur public (art. 2, 1°).

Le projet de loi fait le choix législatif de maintenir la notion de « service public » à l'article 14 L.R&S et d'y ajouter la notion des « autres personnes et organisations qui remplissent un service d'intérêt public général».[22] Il s'ensuit que toutes les instances qui relèvent déjà de la première catégorie – par exemple l'État fédéral, les Communautés, les Régions, les autorités provinciales et locales, ainsi que les centres publics d'aide sociale – ne doivent pas être classées dans la seconde catégorie.
Toutefois, **étant donné que le législateur a précédemment indiqué dans les exposés des motifs que la notion de « tous les services publics » englobe et « doit être comprise dans le sens le plus large possible » (*supra*), et compte tenu du fait que dans la pratique, le besoin se fait ressentir de clarifier davantage cette notion dans la loi, le Comité estime qu'il est préférable d'opter pour un seul concept et de le définir ensuite de manière exhaustive (notamment en précisant toutes les catégories qu'il recouvre, tant sur le plan organique que fonctionnel)(REC-5)**. Vu que la notion de « services publics » est déjà utilisée à l'article 14 L.R&S et vu les passages existants dans les exposés des motifs susmentionnés, il convient de continuer à utiliser cette notion, en y ajoutant une définition exhaustive à l'article 3, point 29°.

À ce titre, il y a donc lieu de mentionner explicitement les autorités publiques relevant de l'État fédéral, des Communautés, des Régions, des autorités provinciales et locales, ainsi que les centres publics d'aide sociale.

La question se pose de savoir si les entités suivantes en font (encore) partie : les zones de secours, les prézones, l'agglomération bruxelloise, les zones intercommunales, les organes territoriaux intra-communaux, la Commission de la Communauté française, la Commission de la Communauté flamande et la Commission communautaire commune.

Enfin, le Comité note que l'article 5 de la Loi relative à la protection des données fait également référence aux ***« personnes morales de droit public qui dépendent de l'Etat fédéral, des entités fédérées ou des autorités locales »*,** et ce indépendamment des catégories déjà visées par le projet d'article 3, 29°. **Le Comité recommande de préciser si ces cas doivent également relever du champ d'application personnel de l'article 14 de la L.R&S (REC-6).**

La notion de « secteur public »

11. L'actuel article 14, dernier alinéa L.R&S stipule ce qui suit :
« Dans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs mission. »

La notion de « service public » n'apparaît qu'à cet endroit dans la Loi Renseignement. **Compte tenu des modifications prévues dans le reste de l'article 14 L.R&S (*supra*), le Comité recommande de préciser cette notion (REC-7).** La question se pose notamment de savoir si le champ d'application personnel entre le pouvoir de réquisition (ex. art. 14, alinéa 2) et le régime d'accès aux bases de données du secteur public (ex. art. 14, dernier alinéa) est le même, en particulier en ce qui concerne les bases de données des services publics au sens fonctionnel.

---

21 Exposé des motifs, p. 27.
22 Passage souligné par le Comité.

Prestataires privés de services de transport et de voyage (art. 18/6/1 L.R&S)

12. Selon l'exposé des motifs, l'article 18/6/1 L.R&S est modifié *« afin de l'aligner sur l'article 14 de la LRS »*. Il est important de noter à cet égard que l'exposé précise que *« les personnes et organisations qui remplissent un service d'intérêt public dans le secteur des transports et des voyages (comme les aéroports) ne relèveront plus du champ d'application de l'article 18/6/1 de la LRS, mais de l'article 14 de la LRS. »*. [23] Il en résulte qu'**une méthode spécifique est transformée en méthode ordinaire.** Concrètement, l'exposé des motifs indique ce qui suit : *« Les données relatives au contrôle de sécurité pour entrer dans la zone « termac » de l'aéroport pourront être demandées sur la base de l'article 14 au lieu de l'article 18/6/1. »*.

Les choix opérés en 2010 par le législateur BIM/MRD d'instaurer dans la Loi Renseignement une structure logique relative aux pouvoirs d'enquête des services de renseignement – à savoir une distinction entre les méthodes exceptionnelles, spécifiques et ordinaires en fonction du degré d'atteinte à la vie privée – est à nouveau abandonnée par la modification législative proposée. Le Comité le regrette. Non seulement cela rend le fonctionnement de ces méthodes de renseignement opaque, mais cela a également pour conséquence une diminution constante des contrôles externes préalables sur le recours à des méthodes intrusives lors de la collecte de données.

13. L'exposé des motifs précise en outre ce qui suit : « *Ce changement ne modifie pas l'application des procédures, autorisations et contrôles prévus actuellement dans la loi organique pour des cas particuliers.* ». Le Comité fait remarquer que ceci est erroné. Vu qu'une méthode spécifique est transformée en méthode ordinaire, **la Commission BIM n'organise plus de contrôle**. De ce fait, **divers mécanismes de contrôle applicables aux méthodes spécifiques sont supprimés.** Ainsi, la Commission BIM ne peut plus mettre fin à une méthode jugée illégale ni suspendre l'exploitation de données collectées illégalement. Comme méthode spécifique, celle-ci ne peut pas non plus être mise en œuvre avant que la décision prise par le dirigeant du service ait été portée à la connaissance de la Commission. Cette notification permet à la Commission d'être informée d'une pratique envisagée et d'intervenir immédiatement si elle estime que cette pratique, qu'elle soit envisagée ou en cours, est illégale. Une notification adressée à la Commission BIM (ou au Comité) après la mise en œuvre de cette méthode ne saurait compenser une telle notification préalable à la Commission BIM.

Dans ce contexte**, le Comité recommande soit de supprimer la modification proposée, soit d'accorder à la Commission BIM une compétence similaire en ce qui concerne les données relatives au transport et au voyage qui sont réclamées en vertu des articles 14 et 16 L.R&S (REC-8).**

En cas d'extension du champ d'application personnel des articles 14 et/ou 16 L.R&S, le Comité est d'avis que, sur ce point également, il convient de solliciter l'avis de l'Autorité de protection des données. En effet, la transmission d'informations par le secteur public ou privé à un service de renseignement constitue un traitement de données à caractère personnel au sens du titre 1 de la Loi relative à la protection des données.

(3) INTELLIGENCE ARTIFICIELLE : DÉVELOPPEMENT ET UTILISATION (projets d'articles 12/1 – 12/5)

Généralités

14. Le Comité constate que les dispositions du projet de loi relatives au développement et à l'utilisation de l'intelligence artificielle par la VSSE et le SGRS dans l'exercice de leurs fonctions sont très succinctes, trop suc-

[23] Exposé des motifs, p. 59.

cinctes en tout cas pour correspondre aux objectifs légitimes formulés dans l'exposé des motifs. Les dispositions des cinq articles concernés ne prévoient en effet que peu de conditions d'application concrètes et de mécanismes de contrôle.

L'exposé des motifs indique que le projet de loi *« poursuit un double objectif : D'une part, promouvoir l'adoption d'une intelligence artificielle axée sur l'humain et digne de confiance, tout en garantissant la protection de la sécurité et des droits fondamentaux des citoyens contre les risques potentiels de l'IA et, d'autre part, soutenir les nécessités opérationnelles des services de renseignement et de sécurité, qui entendent assumer un rôle de premier plan dans le développement et l'utilisation d'une IA sûre, digne de confiance et éthique dans l'exercice de leurs missions. »*.[24] Le Comité salue chaque objectif fixé.

15. Le projet de loi ajoute une définition des **notions de « système d'IA »** (projet d'article 3, 14/1° L.R&S) et **« bac à sable d'IA »** (projet d'article 3, 14°/2 L.R&S), qui s'appuient clairement sur la définition des concepts concernés dans le Règlement de l'Union européenne sur l'IA [25] (art. 3, 1) resp. art. 3, 55) Règlement IA).

L'exposé des motifs indique ce qui suit : *« Bien que le Règlement (UE) 2024/1689 sur l'intelligence artificielle par les services de renseignement et de sécurité dans l'exercice de leurs missions, la définition reprise dans le présent avant-projet s'aligne sur la définition du Règlement sur l'IA ainsi que sur les travaux des organisations internationales œuvrant dans le domaine de l'IA afin de garantir la sécurité juridique, et de faciliter la convergence, tout en offrant la souplesse nécessaire pour tenir compte des évolutions technologiques rapides dans ce domaine. »*.[26]

Le Comité fait remarquer que dans le règlement sur l'IA, les « sous la surveillance réglementaire » ont également été ajoutés à la définition de « bac à sable d'IA ». Au vu de l'exposé des motifs [27] et du projet d'article 12/3, alinéa 2 L.R&S, il est clair que l'auteur souhaite placer le développement de l'IA par les services de renseignement sous la surveillance du Comité R/I. **Pour cette raison, et dans un souci de clarté textuelle, le Comité recommande d'ajouter les mots « sous la surveillance du Comité permanent R » à la définition légale de la notion de « bac à sable d'IA » (REC-9).** Le Comité utilise ici délibérément le terme « contrôle » et non « accompagnement », car il estime qu'un contrôle indépendant est incompatible avec l'accompagnement du processus susmentionné.

16. Sur le plan légistique et sur le fond, le Comité ne comprend pas pourquoi la disposition « Les services de renseignement et de sécurité peuvent développer et utiliser des systèmes d'IA dans l'exercice des missions visées aux articles 7, 8 et 11 » (projet d'article 12/1) et la disposition « Le développement ou l'utilisation de systèmes d'IA n'est autorisé que si les garanties et conditions énoncées aux articles 12/3 à 12/5 sont remplies. » figurent dans deux articles de loi distincts. **Afin de mieux mettre en évidence le lien indissociable qui unit ces deux dispositions, le Comité recommande de les regrouper dans un seul article de loi (REC-10).**

Par ailleurs, le Comité souligne que l'article 8 L.R&S ne reprend aucune mission de la VSSE, mais se borne à donner les définitions légales des notions utilisées dans l'article 7 L.R&S, qui, lui, définit les missions de la VSSE. **Le Comité recommande de remplacer les mots « les articles 7, 8 et 11 » dans le projet d'article 12/1 par « les articles 7 et 11 » (REC-11).**

---

[24] Exposé des motifs, p. 15 (et 36).

[25] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant (…) (Règlement intelligence artificielle), JO L. du 12 juillet 2024.

[26] Exposé des motifs, p. 26.

[27] Exposé des motifs, p. 26 et 37.

Le développement de l'IA et le contrôle externe exercé sur celui-ci

17. Le projet d'article 12/3 L.R&S prévoit ce qui suit : *« Tout système d'intelligence artificielle implémenté par les services de renseignement et de sécurité, doit avoir été testé dans un bac à sable d'IA ou avoir été soumis à toute mesure alternative avant d'être déployé dans des conditions réelles d'utilisation.*
Le dirigeant du service fournit au Comité permanent R la documentation du test ou de la mesure alternative visés à l'alinéa 1er.
Les données à caractère personnel collectées initialement à une autre fin peuvent être traitées pour le développement, l'entrainement et le test de systèmes d'IA dans le bac à sable d'IA. ».

En ce qui concerne le contrôle du Comité mentionné ci-dessus, l'exposé des motifs précise ce qui suit : *« Cette documentation est fournie par le dirigeant du service au Comité permanent R dans le cadre de son contrôle organisé par la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. ».*[28] **Le Comité estime qu'il convient d'ajouter explicitement, tant dans l'exposé des motifs que dans le projet de loi, que le contrôle en question s'effectue en tenant compte des compétences correctrices du Comité tel que visé à l'article 51/3 de la Loi du 18 juillet 1991 (REC-12).** Il s'agit des compétences correctrices dont il dispose dans le cadre de son contrôle du traitement des données à caractère personnel, et qui comprennent notamment le pouvoir d'imposer une limitation ou une interdiction de traitement à l'égard des services de renseignement. Compte tenu notamment du troisième alinéa du projet d'article 12/3, qui prévoit que les services de renseignement peuvent utiliser des données à caractère personnel collectées à d'autres fins, un tel ajout est essentiel.

18. Le projet d'article 12/4 prévoit l'obligation de réaliser une analyse d'impact sur les droits fondamentaux pour chaque utilisation de systèmes d'IA. Il définit également les éléments obligatoires de cette analyse.

Il est à noter que l'élément central d'une telle analyse d'impact, à savoir **« une description des risques spécifiques de préjudice susceptibles d'avoir des conséquences pour les catégories de personnes physiques ou les groupes de personnes physiques potentiellement visés »** fait défaut. Autre exigence, à savoir « une description de la période dans laquelle et la période à laquelle le système d'IA est destiné à être utilisé », à laquelle il manque **« une description de la fréquence à laquelle le système d'IA sera utilisé »**. **Le Comité estime que ces deux aspects doivent être ajoutés (REC-13).**

19. Vu la complexité technique des systèmes d'IA, **le Comité estime que pour pouvoir exercer son contrôle sur un système d'IA, il est nécessaire qu'il reçoive et qu'il ait en tout temps accès aux données introduites par les humains, aux résultats générés par le système et aux mécanismes sous-jacents des technologies d'IA et algorithmiques utilisés**, en particulier et de manière non limitative :

- aux données d'entraînement et aux jeux de données ;
- à la logique du modèle, son architecture et son code source ;
- aux indicateurs de performance ;
- aux journaux (logs) et aux journaux d'audit et de modification du système.

Lorsque des solutions commerciales sont utilisées sur lesquelles les services de renseignements n'ont pas la maîtrise totale, le Comité doit avoir accès au moins aux mêmes informations que les services et disposer d'un environnement bac à sable permettant d'auditer les parcours décisionnels du système (REC-14).

[28] Exposé des motifs, p. 37.

20. Le Comité constate que le principe du **contrôle humain** est introduit dans le projet d'article 12/5, alinéa 1er. Cette disposition stipule ce qui suit : *« Toute utilisation d'un système d'IA est soumise à un contrôle humain afin de réduire ou prévenir tout risque d'atteinte aux droits fondamentaux »*.

Cette disposition limite le contrôle humain dans le cadre de l'utilisation de l'IA, mais il n'existe pas d'obligation similaire en matière de développement de l'IA. Or, ceci est fondamental. **S'inspirant de l'article 14 du Règlement IA, le Comité recommande d'inscrire les principes suivants dans la loi (REC-15)** :

- tout système d'IA mis en œuvre par les services de renseignement et de sécurité est conçu et développé, y compris les outils d'interface homme-machine appropriés, de manière à pouvoir faire l'objet d'un contrôle efficace par des personnes physiques pendant toute la durée de son utilisation ;
- la supervision humaine vise à prévenir ou à limiter les risques pour la sécurité ou les droits fondamentaux qui pourraient survenir lorsqu'un système d'IA est utilisé conformément à sa finalité prévue ou dans une situation d'utilisation abusive raisonnablement prévisible ;
- les mesures de contrôle sont garanties par des dispositifs qui, lorsque cela est techniquement possible, sont intégrés au système d'IA avant sa mise en service ;
- afin de mettre en œuvre les aspects susmentionnés, le système d'IA doit être conçu de manière à permettre aux personnes physiques chargées de la supervision humaine d'intervenir de manière appropriée et proportionnée :
  a) bien comprendre les capacités et les limites pertinentes du système d'IA et être en mesure d'en surveiller correctement le fonctionnement, notamment en vue de détecter et de traiter les irrégularités, les dysfonctionnements et les performances inattendues ;
  b) rester conscient de la tendance potentielle à se fier automatiquement ou excessivement aux résultats d'un système d'IA ;
  c) interpréter correctement les résultats d'un système d'IA à haut risque, par exemple les outils et méthodes disponibles pour cette interprétation ;
  d) pouvoir décider, dans toutes les situations spécifiques, de ne pas utiliser le système d'IA ou d'ignorer d'une autre manière les résultats du système d'IA présentant un risque élevé, en les remplaçant par une autre décision ou en les annulant ;
  e) intervenir dans le fonctionnement du système d'IA ou interrompre le système à l'aide d'un bouton d'arrêt ou d'une procédure similaire permettant d'arrêter le système en toute sécurité.

L'utilisation de l'IA et le contrôle externe exercé sur celle-ci

21. Le Comité constate que le projet de loi ne contient pas de dispositions spécifiques adaptées aux différents types d'utilisation de l'IA dans le cadre de l'exécution des missions. Ainsi, l'utilisation de l'IA n'est pas seulement possible dans le cadre de la collecte d'informations, mais aussi dans le cadre de l'analyse du renseignement (par exemple l'évaluation des personnes physiques). Le projet de loi autorise également, de manière indirecte, l'utilisation de l'IA dans le cadre d'actions d'entrave (*infra*). **Le Comité considère que la loi devrait prévoir des mécanismes de contrôle spécifiques concernant cette utilisation de l'IA, la Commission BIM et le Comité R/I disposant de compétences correctrices en cas d'utilisation abusive (par exemple sur la base de l'IA, une personne est qualifiée de dangereuse, alors qu'aucune information objective ne vient étayer cette conclusion) (REC-16).**

22. La définition du système d'IA n'exclut pas le recours à de l'IA agentique, caractérisé par une autonomie et une capacité d'action sur l'environnement réel plus élevées. Ce type d'IA peut générer des données et des actions de manière massive, même sous supervision humaine. Le risque est réel que le contrôle externe et indépendant du Comité, que ce soit en temps réel ou a posteriori, ne puisse être effectivement réalisé. Une solution possible est l'implantation, au sein du système IA même, de mécanisme de monitoring, de rapportage et de contrôle, basé également sur l'IA et sous contrôle du Comité. Ce problème, particulièrement présent pour les systèmes agentiques, demeure pour tout système d'IA. Le changement d'échelle dans l'activité contrôlée

doit pouvoir être accompagné, lorsque c'est nécessaire, par un changement d'échelle dans les modalités du contrôle.
Le Comité recommande donc que le projet prévoie le pouvoir d'installer, sur décision motivée du Comité, des modules de contrôle des systèmes d'IA. Chaque système étant différent, la solution technique pour le module de contrôle doit être discutée de bonne foi entre le Comité et le service contrôlé. Parmi les exemples de techniques possibles figurent les interfaces de programmation d'application (API), les *« trusted exécution environments »* ou les modules *« sidecar »*.
Lorsque des solutions commerciales sont utilisées, les contrats de service ou les licences d'utilisation doivent inclure une clause obligeant le partenaire privé à accepter l'installation de modules de surveillance par l'autorité de contrôle (REC-17).

(4) COMMISSION D'INFRACTIONS

Contraventions, faits punissables de SAC et Code de la route (art. 13/1 L.R&S)

23. Concernant l'article 13/1 L.R&S, l'expositif des motifs indique ce qui suit [29] : *« Dans l'article 13/1, plusieurs modifications ont été apportées.*
Tout d'abord, le champ d'application du deuxième paragraphe de l'article 13/1 est adapté. Jusqu'à présent, les agents pouvaient commettre des contraventions, des infractions au code de la route et des vols d'usage si cela était absolument nécessaire afin d'assurer l'exécution optimale de la mission ou de garantir leur propre sécurité ou celle de tiers. Ces infractions ne peuvent être commises que lorsque les agents sont chargés de l'exécution des méthodes de recueil de données ou lorsqu'ils sont membres de l'équipe d'intervention. La modification vise à actualiser les infractions pouvant être commises par les agents des services de renseignement et de sécurité au regard du nouveau Code pénal.
Les faits punissables de SAC sont ajoutés aux faits pouvant être commis. Dans la pratique, ces infractions mineures se produisent en effet dans des situations où les services de renseignement et de sécurité doivent pouvoir agir rapidement. Bien que ces faits aient une gravité juridique limitée, ils jouent de plus en plus souvent un rôle opérationnel important. ».[30]

24. Tout d'abord, le Comité fait remarquer que dans l'article 13/1, le mot **« contraventions »** n'a pas été supprimé. **Ceci doit être fait (REC-18)**, étant donné que le nouveau Code pénal a soit supprimé les infractions existantes, soit les a requalifiées en infractions relevant du niveau de peine 1. Si le rédacteur souhaite que certaines de ces infractions, reclassées en infractions de niveau 1, puissent également faire l'objet à l'avenir d'un motif d'exonération excluant toute peine, les articles concernés du nouveau Code pénal doivent être explicitement énumérés à l'article 13/1.

25. Deuxièmement, le Comité constate qu'il est proposé d'ajouter la notion de **« faits punissables SAC »** à l'article 13/1 L.R&S. Il convient de noter d'emblée que le Comité **ne partage pas l'avis exprimé dans l'exposé des motifs selon lequel les faits punissables SAC seraient de simples infractions mineures**, dont la gravité juridique est limitée. À la faveur des différentes modifications apportées à la loi relative aux SAC et à la Loi sur la circulation routière, les communes ont également obtenu le pouvoir de sanctionner certaines infractions par une amende SAC. Compte tenu des peines, il ne s'agit pas d'infractions mineures.

En outre, le Comité attire l'attention sur le fait que **la notion de « faits punissables SAC »** n'est pas une notion juridique clairement définie (contrairement à la notion de vol par usage, qui renvoie clairement à l'article 461, alinéa 2, du Code pénal - 1867). De ce fait, le simple ajout de la notion de « faits punissables SAC » à l'article

[29] Exposé des motifs, p.. 39-40.
[30] Passages soulignés par le Comité.

13/1 L.R&S ne suffit pas. **Il convient de préciser pour quelles infractions exactement un motif d'exonération de peine est introduit pour les agents (REC-19).**

Dans ce cadre, l'article 29 § 2, alinéa 2 de la Loi relative à la police de la circulation routière est important. Celui-ci stipule ce qui suit : *« Les stationnements à durée limitée, les stationnements payants et les stationnements sur les emplacements réservés aux titulaires d'une carte de stationnement communale définis dans les règlements précités ne sont pas sanctionnés pénalement, sauf le stationnement alterné semi-mensuel, la limitation du stationnement de longue durée et la fraude avec le disque de stationnement. »*. En raison de la dépénalisation des infractions concernées, il ne s'agit plus d'infractions de nature pénale, mais d'**infractions de nature administrative** pouvant être sanctionnées soit par une sanction administrative (ce que l'on appelle une amende SAC), soit par une redevance. **Le mot « peine » dans l'actuel article 13/1 semble donc ne pas suffire pour couvrir ces dernières réactions.**

26. La notion de « faits punissables SAC » est également utilisée dans **les projets d'articles 19/3, § 1er et 19/4**, ce qui, selon le Comité, nécessite donc une modification **(REC-20)**.

27. Enfin, le Comité rappelle que le 1er juin 2027, **le Code de la route** sera remplacé par le Code fédéral de la voie publique, le Code bruxellois de la voie publique, le Code de la route flamand (*Vlaams Verkeersreglement*) et le Code wallon de la voie publique. Ceci est important pour l'article 13/1, § 1er L.R&S. **Compte tenu de cette modification à venir et afin d'améliorer la lisibilité de l'article 13/1, § 1er L.R&S, le Comité suggère d'ajouter la définition suivante à la liste des notions reprises à l'article 3 (REC-21)** :

« Code de la route : le Code fédéral de la voie publique, le Code bruxellois de la voie publique, le Règlement flamand de la circulation (Vlaams Verkeersreglement) et le Code wallon de la voie publique*; »*

Il convient d'ajouter un article à la fin du projet de loi fixant l'**entrée en vigueur** de cette disposition au 1er juin 2027.

L'interdiction des provocations

28. Ceci s'ajoute à l'aspect lié à la commission d'infractions. **Le Comité considère qu'en ce qui concerne les membres du personnel des services de renseignement, il convient d'instaurer une interdiction légale de provocation à commettre des infractions (REC-22)** qui est comparable à l'interdiction légale de provocation à l'égard des agents de police (art. 30 T.P. CIC).

L'article 30 T.P. CIC stipule que :
« Il est interdit de provoquer des infractions.
Il y a provocation lorsque, dans le chef de l'auteur, l'intention délictueuse est directement née ou est renforcée, ou est confirmée alors que l'auteur voulait y mettre fin, par l'intervention d'un fonctionnaire de police ou d'un tiers agissant à la demande expresse de ce fonctionnaire, ou d'un infiltrant civil dans le cadre d'une infiltration civile visée au livre I, chapitre IV, section III sous-section 4bis du Code d'instruction.
En cas de provocation, l'action publique est irrecevable en ce qui concerne ces faits. ».

Une telle interdiction peut être inscrite soit par une modification de l'article 30 T.P. CIC ainsi que dans la Loi Renseignement (par exemple dans un § 5 à ajouter à l'article 13 L.R&S). Étant donné que la Loi Renseignement prévoit *de lege lata* un régime spécifique pour les infractions commises par les services de renseignement et compte tenu de la plus grande visibilité dont bénéficient les membres du personnel de ces services de renseignement, qui sont plus familiarisés avec cette loi, le Comité préfère un ajout dans la Loi Renseignement. En partant de l'article 30 T.P. CIC – cette disposition est en effet conforme à la jurisprudence de la Cour de cassation et de la Cour constitutionnelle en ce qui concerne la définition en question (alinéa 2) et traduit la volonté

du législateur en ce qui concerne la sanction en question (troisième alinéa) – il est préférable de formuler une telle interdiction comme suit :

[Art. 13, § 5]:
« Il est interdit de provoquer des infractions. Il y a provocation lorsque, dans le chef de l'auteur, l'intention délictueuse est directement née ou est renforcée, ou est confirmée alors que l'auteur voulait y mettre fin, par l'intervention d'un agent d'un service de renseignement et de sécurité ou d'un tiers agissant à la demande expresse de ce membre du personnel.
En cas de provocation, l'action publique est irrecevable en ce qui concerne ces faits. ».

29. Selon le Comité, une telle interdiction légale doit être introduite pour diverses raisons. *Premièrement,* le Comité rappelle que l'interdiction légale de provocation à l'égard des agents de police a déjà été instaurée par la Loi relative aux Méthodes particulières de recherche du 6 janvier 2003 (insertion d'un article 47*quater* CIC). Après l'annulation par la Cour constitutionnelle[31] de l'article 47*quater* CIC[32], la Loi de réparation MPR du 27 décembre 2005 a inséré un nouvel article 30 T.P. CIC. Une légère modification a été apportée à la suite de l'introduction d'une réglementation relative à l'infiltration civile. Bien que la Loi MRD du 4 février 2010 a *sensu lato* créé, pour les services de renseignement, des pouvoirs d'enquête similaires aux MPR, l'instauration d'une interdiction similaire concernant l'incitation à commettre des infractions a été omise. Il n'existe toutefois aucune raison objective de fond justifiant qu'une telle interdiction s'applique aux fonctionnaires de police mais pas aux agents des services de renseignement. Cette constatation est d'autant plus vraie aujourd'hui qu'il apparaît que les cibles des services de renseignement évoluent de plus en plus dans un milieu criminel. Cela tient à la fois à la volonté du législateur de lutter par la voie pénale contre certaines menaces pour la sécurité nationale relevant de la compétence de la VSSE et du SGRS, et donc de les ériger en infractions pénales, et à certaines circonstances factuelles elles-mêmes.

Deuxièmement, le Comité rappelle que l'interdiction de commettre des infractions prévue par l'article 13/1, § 1er L.R&S n'est pas suffisante pour couvrir l'interdiction de la provocation. Un moyen utilisé dans le cadre d'une provocation pour susciter, renforcer ou confirmer l'intention criminelle d'une personne ne doit pas nécessairement être constitutif d'une infraction. Il n'est même pas nécessaire qu'il soit illégal ; un moyen fallacieux suffit.

Troisièmement, il est important de noter que les services de renseignement se voient attribuer de plus en plus de compétences dont l'exercice comporte un risque de provocation. Plus précisément, l'octroi aux services de renseignement de pouvoirs étendus en matière d'entrave requiert une interdiction légale explicite de la provocation à commettre des infractions de la part des membres du personnel des services de renseignement. **L'utilisation d'informateurs comme agents d'influence dans le cadre d'une action d'entrave, par exemple, ne doit pas se transformer en une mobilisation d'agents provocateurs.** Bien qu'il puisse exister des raisons légitimes d'accorder davantage de pouvoirs à la VSSE et au SGRS chargés d'entraver les menaces graves, rien ne justifie objectivement le fait de provoquer des infractions pénales dans ce contexte. Non seulement cela serait contraire à l'article 6, alinéa 1er CEDH si les personnes concernées faisaient l'objet de poursuites, mais, dans un État de droit démocratique, l'incitation à commettre des infractions pénales ne saurait tout simplement être légitimée. Pour ces seules raisons, le Comité demande que l'interdiction de provocation susmentionnée soit clairement inscrite dans la Loi Renseignement.

30. Enfin, le Comité rappelle l'arrêt n° 202/2004 de la Cour constitutionnelle du 21 décembre 2004. La Cour n'a pas accepté la différence dans la définition légale de la provocation selon qu'une méthode particulière de

---

31 Cour constitutionnelle, arrêt n° 202/2004 du 21 décembre 2004.

32 La Cour n'a pas accepté la différence dans la définition légale de la provocation selon qu'une méthode particulière de recherche a été utilisée ou non.

recherche a été utilisée ou non. Il faut en déduire que la notion de provocation doit également avoir **une portée générale** à l'égard des services de renseignement et ne peut pas se limiter aux méthodes particulières de renseignement.
Pour ces raisons, le Comité propose d'ajouter, avant le paragraphe proposé ci-dessus, un paragraphe 5 à l'article 13 L.R&S.

Une lacune dans la procédure pénale

31. Le Comité souhaite également attirer l'attention sur une lacune dans la procédure pénale. Dans le cadre de cette procédure, à l'exception d'un cas limité (voir ci-dessous), le juge n'a pas la possibilité de vérifier la légalité d'*une note non classifiée d'un service de renseignement, transmise conformément à l'article 19 L.R&S*[33] *et versée au dossier pénal*, y compris la légalité de la collecte d'informations qui a précédé la rédaction d'une telle note.

La procédure (actuelle) limitée constitue ce qu'on appelle une « procédure d'avis préjudicielle » (*cf*. les articles 131*bis*, 189*quater* en 279*bis* CIC) dans le cadre de laquelle une juridiction pénale peut demander au Comité R/I de vérifier la régularité des méthodes MRD qui ont conduit à l'établissement d'un « procès-verbal non classifié » (*cf*. art. 19/1 L.R&S). Ce procès-verbal est établi par la Commission BIM lorsque des indices d'infractions ont été mis au jour lors de l'utilisation de certaines méthodes MRD. La procédure d'avis préjudicielle est toutefois peu utilisé dans la pratique. Le transfert des données des services de renseignement vers le parquet ne s'effectue que dans des cas exceptionnels par le biais d'un tel procès-verbal. La plupart des informations sont transmises au parquet par le biais d'une note du dirigeant des services de renseignement (sur la base de l'obligation de dénonciation (*cf.* article 29 CIC) ou – essentiellement – la compétence générale de communication (*cf.* article 19 L.R&S).

Le Comité estime que l'absence de contrôle particulier, pendant la procédure pénale, sur l'enquête de renseignement au cours de la procédure pénale peut poser problème lorsqu'un dossier pénal contient des informations provenant d'un service de renseignement qui ont été obtenues par le recours illicite à des méthodes ordinaires (par exemple en recourant à des méthodes ordinaires alors qu'il aurait fallu suivre la procédure MRD) ou qui contient un traitement illicite de données à caractère personnel (par exemple qualifier une personne de dangereuse alors que cela n'est pas étayé par les informations requises). Dans ce contexte, le Comité recommande **de généraliser la « procédure d'avis préjudicielle en matière pénale » (REC-23)**. À cet égard, les juridictions pénales doivent avoir la possibilité de saisir le Comité et de l'interroger sur la légalité de toutes les informations non classifiées provenant des services de renseignement qui ont été transmises sur pied de l'article 19 de la Loi de 30 novembre 1998 et qui figurent dans le dossier pénal.

(5) OPEN SOURCES (projet de paragraphe 3 à l'article 16/1 L.R&S)

32. Un troisième paragraphe est ajouté à l'article 16/01 L.R&S :
« Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent traiter toutes informations et données à caractère personnel transitant dans les lieux accessibles au public des systèmes informatiques et de communications y compris celles qui ont été obtenues par la commission d'infractions, que des formalités doivent être accomplies ou non pour y accéder. »

[33] Cette disposition prévoit une compétence générale des services de renseignement de communiquer des informations.

La disposition en question crée une base juridique pour *« traiter les données accessibles en open sources mais qui ont été obtenues par la commission d'infractions (Leaks-DB, Darknet) »*[34], par exemple par un lanceur d'alerte d'un service de renseignement étranger.

33. Le Comité propose **d'apporter les améliorations suivantes (REC-24)** :
« Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, collecter, enregistrer et traiter toutes les informations et données à caractère personnel transmises par le biais de parties accessibles au public de systèmes informatiques et de communication, y compris les informations et données à caractère personnel obtenues par la commission d'infractions pénales par des tiers, indépendamment de la nécessité pour les services de renseignement et de sécurité d'accomplir des formalités pour y avoir accès. ».

Le Comité constate en effet que la disposition actuelle est difficile à comprendre et peut poser un problème d'interprétation. Le Comité propose l'amélioration susmentionnée. La plupart des modifications consistent en de simples **corrections linguistiques** dans la version néerlandaise de la disposition en question et en des adaptations tenant compte de la manière dont d'autres articles de loi décrivent les méthodes (notamment la phrase liminaire de la disposition).

Le terme **« traiter »** est défini comme **« collecter, enregistrer et traiter »**. L'ajout du terme « collecter » indique clairement qu'il s'agit d'une méthode de renseignement ; le projet de loi place en effet la disposition en question dans la sous-section qui règle les méthodes de renseignement ordinaires. L'ajout du terme « enregistrer » précise qu'une compétence spécifique en matière de conservation y est également associée. Imaginons qu'un lanceur d'alerte d'un service de renseignement étranger publie sur Internet un document détaillé (il s'agit donc *de jure* d'un fichier de données). Dans un tel cas, il va de soi que la VSSE et le SGRS ne se contenteront pas de récupérer ce fichier le plus rapidement possible – le document pouvant en effet avoir déjà été supprimé le lendemain – mais souhaiteront également l'intégrer à une base de données interne (« enregistrer »). Dans une phase ultérieure, le service de renseignement devra déterminer quelles données sont réellement pertinentes pour l'exercice de ses fonctions, et seules ces données pourront être conservées dans la base de données centrale. Le terme « traitement » est conservé, mais le fait de le placer en dernière position indique clairement qu'il revêt une acception générique, au sens des articles 26, 2°, et 72, § 1er, de la Loi du 30 juillet 2018 relative à la protection des données.

34. L'auteur du projet **doit prévoir un mécanisme permettant aux services de respecter l'article 2, § 2 L.R&S - relatif au traitement des données protégées par le secret professionnel des avocats, des médecins et des journalistes – lorsque des données visées à l'article 16/1 sont traitées. Le Comité recommande, par exemple, de fixer un délai maximal dans lequel le service doit effacer les données qu'il n'est pas autorisé à traiter** (**REC-25**).

34bis. Les services de renseignement ont de plus en plus souvent recours à des **données disponibles dans le commerce et accessibles au public** (ce que l'on appelle les *commercially and publicly available data*), sans bénéficier des garanties juridiques traditionnelles qui s'appliquent à la collecte et au traitement classiques des données. C'est ainsi que les services obtiennent une quantité croissante de données à caractère personnel par l'intermédiaire de courtiers en données, d'ensembles de données achetés (y compris issus de fuites de données), d'outils d'analyse commerciaux, de l'intelligence open source (OSINT) et de transferts volontaires de données par des entreprises privées. **Les services de renseignement dépendent donc de moins en moins des méthodes de renseignement classiques et recourent de plus en plus à des sources de données commerciales.** Comme cette collecte d'informations n'est généralement pas soumise à des obligations légales, ces activités de renseignement échappent souvent à tout contrôle externe. Il en résulte un angle mort de plus en plus important dans le contrôle démocratique. **Le Comité reconnaît que, dans certains cas et sous certaines**

[34] Exposé des motifs, p. 50.

conditions, il peut être utile pour la VSSE et le SGRS d'acheter des données (à caractère personnel) auprès de courtiers en données. Dans le même temps, le Comité constate qu'il n'existe actuellement pas suffisamment de garanties juridiques dans le cadre de cette forme de collecte et de traitement des informations. À l'heure actuelle, le Comité ne dispose pas non plus des instruments juridiques nécessaires pour exercer un contrôle efficace et efficient sur cette forme de collecte et de traitement des informations. **Le Comité recommande dès lors de mettre en place un cadre juridique clair réglant l'achat et le traitement des données commerciales** (par exemple des analyses de risques obligatoires concernant la vie privée et d'autres droits fondamentaux, des procédures de conformité obligatoires, une interdiction de certaines utilisations discriminatoires des données achetées), **avec une autorisation préalable pour les formes de collecte de données à haut risque, et un contrôle indépendant exercé par le Comité.** De plus, selon le Comité, il faudrait instaurer une interdiction légale empêchant les services de renseignement d'acheter des données à caractère personnel pour lesquelles ils ont normalement besoin d'une autorisation de la Commission BIM, ou imposer l'obligation de n'acheter de telles données qu'après avoir obtenu une telle autorisation préalable. **Enfin, le Comité plaide vivement pour que des décisions contraignantes puissent être prises afin de supprimer des ensembles de données ou d'annuler un achat en cas d'illégalité avérée** (**REC-25bis**).

(6) ACCÈS AUX BASES DE DONNÉES DE L'UE (projet d'article 16/3/2 L.R&S), ETIAS ET EURODAC

35. Le Comité constate que le projet d'article 16/3/2 L.R&S instaure un droit d'accès à l'EES (Entry/Exit System)[35], le système dit « d'entrée et de sortie » de l'UE destiné à prévenir, détecter ou enquêter sur les infractions terroristes et autres infractions pénales graves.

Le Comité constate également que le projet d'article 16/3/2 est fondé sur l'actuel article 16/3/1, qui établit un droit d'accès au système ETIAS (European Travel Information and Autorisation System) [36].

Le Comité rappelle qu'il a récemment rendu un avis législatif [37] concernant l'instauration d'un droit d'accès pour les services de renseignement à Eurodac (European Asylum Dactyloscopy)[38]. Il s'agit d'une base de données gérée au niveau central par l'Union européenne. Concrètement, c'est l'Agence de l'Union européenne pour la gestion des systèmes d'information à grande échelle au sein de l'espace de liberté de sécurité et de justice (eu-LISA) qui en assure la gestion opérationnelle et technique. Dans l'avis précité, le Comité indique ce qui suit : *« Le Comité est favorable à une compétence d'accès pour la Sûreté de l'État (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS), à condition toutefois que la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) ajoute les conditions et procédures nécessaires à l'exercice de*

---

35 Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives (…), JO UE 9 décembre 2017, L 327/20.

36 Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (Etias) (…), JO UE 19 septembre 2018, L 236/1.

37 Avis n° 2026/003 du 10 février 2026 du Comité R/I concernant « le projet de loi modifiant la loi sur les étrangers : accès à Eurodac pour la VSSE et le SGRS » (www.comiteri.be).

38 Règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'« Eurodac » pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/1351 et (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n° 603/2013 du Parlement européen et du Conseil, *JO* L du 22 mai 2024.

cette compétence. Eurodac contient en effet des données à caractère personnel sensibles, notamment des données biométriques (empreintes digitales, image faciale). L'exercice de cette compétence d'accès par la VSSE et le SGRS requiert également un contrôle externe accru. ».

36. Étant donné que EES, ETIAS et EURODAC sont trois bases de données de l'UE, que, dans le présent projet de loi, l'auteur exprime clairement sa volonté de soumettre EES et ETIAS à une même procédure, que le projet d'article 16/3/2 prévoit la même procédure que l'actuel article 16/3/1 et compte tenu de l'avis susmentionné du Comité (*supra*), **le Comité estime qu'il est préférable de remplacer et de généraliser l'actuel article 16/3/1 L.R&S**, qui règle actuellement l'accès au système ETIAS **(REC-26)**, comme expliqué ci-après (*les modifications et ajouts par rapport à l'article actuel sont indiqués en gras ; des précisions à ce sujet suivront*).

L'objectif général du nouvel article 16/3/1 L.R&S est de **définir de manière générale les conditions de fond et de forme applicables à l'exercice d'un droit d'accès par la VSSE et le SGRS à une base de données de l'UE gérée de manière centralisée**[39], à laquelle les services de renseignement ont accès et qui contient des données à caractère personnel intrusives similaires. Cela implique toutefois d'apporter un certain nombre de modifications à l'actuel article 16/3/1 L.R&S – et, par conséquent, également au projet d'article 16/3/2 L.R&S – que le Comité estime nécessaires au regard d'un contrôle indépendant.

Article 16/3/1.[40]

---

[39] Par exemple, cela ne s'applique donc pas à l'accès aux données PNR, tel que prévu à l'article 16/3 L.R&S.

[40] L'actuel article 16/3/1 stipule que :
§ 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, décider de façon dûment motivée d'accéder aux données conservées dans le système central ETIAS conformément à l'article 13 de la loi du 29 mars 2024 relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.).
§ 2. A l'exception des cas visés aux paragraphes 4 et 5, la méthode visée au paragraphe 1er peut seulement être mise en œuvre après que le président de la Commission, ou un autre membre si le président n'est pas immédiatement disponible, a procédé à un contrôle préalable de la décision écrite et motivée du dirigeant du service concerné ou de son délégué.
La décision du dirigeant du service concerné ou de son délégué mentionne :
1° les personnes physiques qui font l'objet de la méthode ;
2° les circonstances de fait qui justifient la méthode ainsi que la motivation relative à la nécessité et à la proportionnalité;
3° l'indication, dûment motivée, du lien direct entre les missions visées aux articles 7, 8 et 11 de la présente loi et les finalités mentionnées à l'article 13, § 1er, de la loi du 29 mars 2024 relative à l'établissement et à l'organisation des missions de l'unité nationale ETIAS (U.N.E.) ;
4° le cas échéant, les raisons qui justifient l'urgence ;
5° le cas échéant, la justification de la nécessité de consulter certaines données du système central ETIAS.
Les mentions visées au deuxième alinéa sont prescrites à peine d'illégalité.
§ 3. Le président de la Commission, ou un autre membre si le président n'est pas immédiatement disponible, adresse au dirigeant du service concerné ou son délégué une réponse écrite au plus tard le premier jour ouvrable après réception de la décision visée au paragraphe 2.
La Commission transmet sans délai au Comité permanent R tous les documents visés aux paragraphes 2 et 3.
§ 4. Si le président de la Commission, ou un autre membre si le président n'est pas immédiatement disponible, transmet une réponse écrite négative ou n'émet pas de réponse écrite dans le délai visé au paragraphe 3, alinéa 1er, le dirigeant du service concerné, ou son délégué, peut saisir le Comité permanent R, qui se prononce dans les plus brefs délais sur la mise en œuvre de la méthode de recueil des données. Le Comité permanent R communique sa réponse au dirigeant du service concerné ou son délégué et à la Commission.
§ 5. En cas d'urgence nécessitant de prévenir un risque imminent pour la vie d'une personne, le dirigeant du service concerné ou son délégué peut autoriser verbalement la méthode après avoir obtenu une réponse verbale positive du président de la Commission, ou d'un autre membre si le président n'est pas immédiatement disponible. Cette décision verbale est confirmée par une décision écrite motivée contenant les mentions visées au paragraphe 2, qui doit parvenir au siège de la Commission au plus tard le premier jour ouvrable suivant la date de la décision verbale.
§ 6. Dès que la décision du dirigeant du service concerné ou son délégué est approuvée par écrit par la Commission ou le Comité permanent R, sont transmis par écrit ou voie électronique au point d'accès central les éléments nécessaires au

« § 1. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, décider de façon dûment motivée d'accéder aux données conservées dans ***les bases de données de l'UE gérées de manière centralisée pour laquelle les services de renseignement et de sécurité disposent d'un droit d'accès ont accès, parmi lesquelles*** *:*
- le système central ETIAS conformément à l'article 13 de la loi du 29 mars 2024 relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) ;
- le système Eurodac conformément à l'article 8septies, § 2, alinéa 1er, 2° et 3° de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers ;
- le système EES conformément à l'article 2/2, § 1er, alinéa 2 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.

§ 2. A l'exception des cas visés aux paragraphes 4 et 5, la méthode visée au paragraphe 1er peut seulement être mise en œuvre après que le président de la Commission, ou un autre membre si le président n'est pas immédiatement disponible, a procédé à un contrôle préalable de la décision écrite et motivée du dirigeant du service concerné ou de son délégué. ***Le contrôle préalable consiste à vérifier que toutes les conditions légales requises pour la collecte des données concernées sont remplies.***

La décision du dirigeant du service concerné ou de son délégué mentionne :
1° les personnes physiques qui font l'objet de la méthode ;
2° les circonstances de fait qui justifient la méthode ainsi que la motivation relative à la nécessité et à la proportionnalité ;
3° l'indication, dûment motivée, ***du lien direct entre les missions visées aux articles 7 et 11 de la présente loi et les finalités prévues par la législation européenne et nationale applicable*** *;*
4° le cas échéant, les raisons qui justifient l'urgence
5° le cas échéant, la justification de la nécessité de consulter certaines données des ***bases de données centrales concernées de l'UE****.*
Les mentions visées au deuxième alinéa sont prescrites à peine d'illégalité.
§ 3. Le président de la Commission, ou un autre membre si le président n'est pas immédiatement disponible, adresse au dirigeant du service concerné ou son délégué une réponse écrite au plus tard le premier jour ouvrable après réception de la décision visée au paragraphe 2.
La Commission transmet sans délai au Comité permanent R tous les documents visés aux paragraphes 2 et 3.

§ 4. Si le président de la Commission, ou un autre membre si le président n'est pas immédiatement disponible, transmet une réponse écrite négative ou n'émet pas de réponse écrite dans le délai visé au paragraphe 3, alinéa 1er, le dirigeant du service concerné, ou son délégué, peut saisir le Comité permanent R, qui se prononce dans les plus brefs délais sur la mise en œuvre de la méthode de recueil des données. Le Comité permanent R communique sa réponse au dirigeant du service concerné ou son délégué et à la Commission. ***La décision du Comité n'est pas susceptible d'appel****.*

§ 5. En cas d'urgence nécessitant de prévenir un risque imminent pour la vie d'une personne, le dirigeant du service concerné ou son délégué peut autoriser verbalement la méthode après avoir obtenu une réponse verbale positive du président de la Commission, ou d'un autre membre si le président n'est pas immédiatement disponible. Cette décision verbale est confirmée par une décision écrite motivée contenant les mentions visées au paragraphe

---

contrôle qu'il doit opérer en vertu de l'article 14, § 1er, de la loi du 29 mars 2024 relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.).
§ 7. La Commission et le Comité permanent R peuvent à tout moment contrôler la légalité de la méthode de recueil de données, en ce compris les principes prévus à l'article 13, et interdire aux services de renseignement et de sécurité l'exploitation des données obtenues dans des conditions qui ne respectent pas les dispositions légales en vigueur.
Si le Comité permanent R constate que les données ont été recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur, il ordonne leur destruction. Dans ce cas, le point d'accès central en est tenu informé.

2, qui doit parvenir au siège de la Commission au plus tard le premier jour ouvrable suivant la date de la décision verbale.

§ 6. Dès que la décision du dirigeant du service concerné ou son délégué est approuvée par écrit par la Commission ou le Comité permanent R, ***un courrier du dirigeant du service ou de son délégué*** *est transmis par écrit ou voie électronique* ***au point d'accès national/central concerné, avec les données demandées***. ***Ce courrier mentionne l'accord préalable de la Commission BIM ou du Comité permanent R.***

§ 7. La Commission et le Comité permanent R peuvent à tout moment contrôler la légalité de la méthode de recueil de données, en ce compris les principes prévus à l'article 13, et interdire aux services de renseignement et de sécurité l'exploitation des données obtenues dans des conditions qui ne respectent pas les dispositions légales en vigueur.
Si le Comité permanent R constate que les données ont été recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur, il ordonne leur destruction. Dans ce cas, ***le point d'accès national/central*** *en est tenu informé. ».*

37. Le Comité utilise l'actuel article 16/3/1 L.R&S comme point de départ, et ce pour plusieurs raisons.

Comme indiqué précédemment, l'article actuel règle les conditions d'accès de la VSSE et du SGRS à ce que l'on appelle les données ETIAS (European Travel Information and Autorisation System), c'est-à-dire les informations relatives au voyage des ressortissants de pays exemptés de visa). ETIAS et Eurodac sont comparables, compte tenu de la nature similaire des données accessibles et du degré équivalent de l'atteinte à la vie privée.

Le Comité constate **que les services de renseignement ne sont actuellement pas énumérés à l'article 2/2 de la Loi sur les étrangers et ne disposent dès lors pas de droit d'accès à la base de données EES**. Dans cette disposition, le législateur habilite le Roi à accorder un tel droit d'accès à d'autres institutions publiques.
Le Comité constate que le système EES, à l'instar d'Eurodac et d'ETIAS, est une base donnée européenne centralisée qui contient des données présentant un respect égal de la vie privée. **Selon le Comité, un droit d'accès aux services de renseignement éventuellement établi par le Roi ne pourrait donc pas non plus être mis en place sans que le législateur ne fixe des conditions matérielles et formelles.**

Comme dans la Loi du 16 mai 2024[41], qui a introduit l'actuel article 16/3 L.R&S réglant le droit d'accès des services de renseignement aux données des passagers, tel que prévu à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers, la loi du 29 mars 2024[42] qui a introduit l'actuel article 16/3/1 L.R&S, s'est fondée sur les motifs pour lesquels la Cour constitutionnelle avait annulé une version antérieure de l'article 16/3 de la Loi du 30 novembre 1998 (voir arrêt n° 131/2023 du 12 octobre 2023). Au cœur de l'argumentation de la Cour figure le fait que l'accès à la base de données en question est possible, mais à la condition stricte d'un accord préalable d'une instance judiciaire ou d'une autorité de contrôle indépendante. Dans les articles 16/3 et 16/3/1, cette compétence – en ce qui concerne la VSSE et le SGRS – a été attribuée à la Commission BIM. En l'absence d'accord de la Commission BIM ou en appel, l'accord préalable du Comité R/I est requis.

38. Selon le Comité, les modifications suivantes apportées à l'article actuel 16/3/1 L.R&S – et donc aussi au projet d'article 16/3/2 L.R&S – sont toutefois nécessaires.

[41] Loi du 16 mai 2024 modifiant la loi du 25 décembre 2016 relative au traitement des données des passagers.
[42] Loi du 29 mars 2024 relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.).

Une première modification importante a été apportée au paragraphe 6. Ce paragraphe porte en effet atteinte au système de contrôle externe de la légalité des méthodes de renseignement réglées par la Loi du 30 novembre 1998. Comme indiqué ci-dessus, il incombe à la Commission BIM, et le cas échéant au Comité R/I, de procéder à un contrôle de légalité du projet de décision visant à collecter les données concernées (c'est-à-dire les données Eurodac, ETIAS et EES). Une fois jugée légale, la décision ne relève plus d'une autorité administrative externe (c'est-à-dire la police intégrée concernant les données Eurodac[43]; le service ETIAS du NTTC au Centre de crise National concernant les données ETIAS) pour remettre en cause cette décision.

Comme le précise la disposition concernée, le Comité R/I intervient dans cette procédure en l'absence de décision de la Commission BIM ou en appel. Une décision du Comité en la matière relève de la compétence juridictionnelle. Une annulation de la décision de la police intégrée reviendrait à – et revient, en ce qui concerne l'intervention du NTTC dans la collecte de données ETIAS – à prendre une décision administrative qui annule une décision judiciaire, et ce dans le cadre d'un contrôle de légalité.[44] **Le Comité insiste donc vivement pour que l'actuel paragraphe 6 soit révisé (REC-27).**

Le paragraphe 2 précise la mission de la Commission BIM, et le cas échéant du Comité R/I, telle qu'elle s'applique actuellement. Un contrôle de légalité consiste à vérifier toutes les exigences légales relatives à la collecte des données concernées, tant celles prévues par la Loi du 30 novembre 1998 que les conditions d'application spécifiques prévues par les réglementations nationales et européennes.

Le paragraphe 6 précise, en outre, qu'aucun recours n'est possible contre une décision du Comité. Une fois que le Comité a établi, sur le plan juridictionnel, que le projet de décision du dirigeant de service ou de son délégué est légal, comme cela a été précisé, une autorité administrative externe ne pourrait en décider autrement. Cette disposition est basée sur l'article 43/8 de la Loi du 30 novembre 1998.

(7) IMAGES NON SENSIBLES AU REGARD DE LA VIE PRIVÉE (projet d'article 16/7 L.R&S)

39. Un nouvel article 16/7 L.R&S est ajouté :
Alinéa 1er : « *Par dérogation aux articles 18/4 et 18/11, dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent prendre des images fixes ou animées pour autant que ces images ne permettent pas, par elles-mêmes, d'identifier une personne physique.* »

L'exposé des motifs précise ce qui suit : « *Le présent projet introduit une nouvelle méthode ordinaire afin de permettre aux services de renseignement et de sécurité de prendre des images fixes ou animées de lieux stratégiques, tels que des infrastructures militaires, industrielles ou de transport, sans recourir aux méthodes spécifiques ou exceptionnelles prévues par la loi organique. Cette approche se justifie par l'absence d'atteinte à la vie privée lorsque ces images ne permettent pas, à elles seules, d'identifier des personnes physiques, l'objectif étant de surveiller des zones ou des installations et non des individus. L'accès rapide à ces images, notamment satellitaires, est essentiel pour anticiper des menaces, soutenir des opérations ou réagir à des situations d'urgence, comme l'ont montré la traque de Jürgen Conings ou la gestion des inondations de 2021. L'introduction de cette méthode*

[43] L'Autorité de protection des données (APD) affirme elle aussi que la police intégrée n'est pas indiquée comme autorité de contrôle. L'APD affirme plus précisément que « *[l]a désignation de la police intégrée ne répond pas aux conditions d'indépendance et d'impartialité (dont notamment l'absence de conflit d'intérêt avec les unités opérationnelles qui solliciteront les demandes d'accès à Eurodac), requises par l'article 6 du règlement Eurodac (…)* ». Avis n° 47/2026 du 17 mars 2026 sur l'avant-projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers en vue de la mise en œuvre du Pacte sur la migration et l'asile de l'Union européenne (CO-A-2025-219), p. 14, 17, 18 et 36. Cet avis a été publié sur le site internet de la Chambre comme *Doc. parl.* Chambre 2025-2026, n° 56-1401/002.

[44] Le Comité considère dès lors que l'actuel paragraphe 6 de l'article16/3/1 L.R&S est inconstitutionnel.

ordinaire permettra aux services de renseignement et de sécurité de renforcer leur efficacité opérationnelle tout en garantissant le respect des droits fondamentaux des personnes physiques. ».[45]

40. Cette disposition pose plusieurs problèmes. **Il convient tout d'abord de préciser le champ d'application territorial de la méthode.** D'une part, cette disposition ne permet pas de déterminer clairement si la VSSE peut la déployer en dehors du territoire, mais à partir de celui-ci (par exemple en contrôlant un drone ou un satellite). La nouvelle méthode ordinaire est en effet créée en référence aux méthodes spécifiques et exceptionnelles prévues aux articles 18/4 et 18/11. Ces dernières méthodes peuvent être mises en œuvre par la VSSE dans l'exercice de certaines missions « sur ou à partir du territoire du Royaume ». En ce qui concerne le SGRS, le Comité R/I constate que cette nouvelle méthode vide en partie de sa substance la compétence propre au SGRS de prise d'images à l'étranger (art. 44/2 L.R&S). Cette dernière disposition continuera de s'appliquer uniquement aux images prises à l'étranger et permettant par elles-mêmes, d'identifier une personne physique. Mais pour les images prises en Belgique ou à l'étranger qui ne permettent pas, à elles seules, de procéder à une identification, c'est l'article 16/7 qui s'appliquera. L'attention du législateur est attirée sur ce fait. **Le Comité recommande de clarifier ce point (REC-28).**

41. Ensuite, le critère d'identification possible d'une personne physique par les images elles-mêmes est ambigüe et inapplicable. Une image est toujours utilisée dans un contexte et en conjonction avec d'autres données. L'exemple choisi dans l'exposé des motifs de la traque de Jürgen Conings est justement un exemple curieux d'images ne permettant pas d'identifier quelqu'un : en prenant des images aériennes des bois où il était recherché, le but était justement de pouvoir l'identifier avec une certaine précision. On peut supposer que les enquêteurs recherchaient un individu isolé et en fuite, plutôt qu'un large groupe de promeneurs accompagné d'animaux ou un groupe d'enfants à vélo. De même, la prise d'image satellitaires de faible résolution permet également d'identifier des individus. Si un véhicule est repéré devant une maison de manière régulière, ou si l'on sait qu'il appartient à un individu déterminé, la présence de ce véhicule dans un autre lieu est un bon indice que la personne en question s'y trouve. Par inférence, on a identifié la personne, même si l'image ne permet pas de le faire à elle seule.
On comprend donc qu'une image est toujours mise en contexte, croisée avec des données ou comparée avec une image d'une personne identifiée mais qu'en soi, elle ne permet que rarement d'identifier «à elle seule » une personne. Vu que l'identification d'une personne (le cas échéant de manière probable) dépend du contexte et d'autres données, il semble impossible au Comité de savoir à l'avance si une image permettra d'identifier un individu. **Le Comité ne s'oppose pas, en soi, à ce que certaines prises d'images fassent l'objet du régime prévu à l'article 16/7 en projet mais recommande d'en clarifier le critère essentiel.**

En résumé, le Comité souligne que, conformément à la législation relative à la protection des données, on est déjà en présence de données à caractère personnel dès lors qu'une personne physique est *identifiable*. **Souvent, les images qui «*ne suffisent pas à elles seules à identifier une personne physique*» constituent déjà des données à caractère personnel (par exemple des images d'un groupe de manifestants), et par conséquent, *« la prise »* de telles images constitue déjà un traitement de données à caractère personnel, et elles ne doivent pas être incluses dans cette nouvelle compétence accessible à tous. Au regard de cette considération, le Comité insiste pour qu'une modification textuelle soit apportée au projet de loi** Conformément aux autres articles de la Loi Renseignement, le Comité propose ,en outre, **dans la version néerlandaise, de remplacer le mot *« mogen »* par *« kunnen »* (REC-29).**

42. Alinéa 2 :
« Les deux services de renseignement et de sécurité tiennent un registre de toutes les prises d'images réalisées conformément à l'alinéa précédent. Le service de renseignement et de sécurité concerné transmet chaque mois

[45] Exposé des motifs, p.15.

au Comité permanent R une liste des prises d'images. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les prises d'images réalisées dans des conditions qui ne respectent pas les dispositions légales. ».

Comme prévu à l'article 16/3, § 7, à l'article 16/3/1, § 7 et dans le projet d'article 16/3/2, § 7, le Comité suggère **l'ajout de la phrase suivante (REC-30) : *« Lorsque le Comité permanent R constate que les données ont été collectées dans des conditions non conformes aux dispositions légales en vigueur, il ordonne leur destruction. ».***

43. Le Comité propose, par ailleurs, d'**ajouter cette phrase dans les dispositions similaires – articles 16/4, § 2, alinéa 4, et § 3, alinéa 4, et article 16/6, § 3 (REC-31)** – où une compétence a également été attribuée au Comité pour prononcer une interdiction d'exploitation, mais où, lors de travaux législatifs antérieurs, l'ajout de l'ordonnance de destruction y afférente a été oublié.

(8) UTILISATION DE MÉTHODES DE RENSEIGNEMENT POUR DES RAISONS DE SÉCURITÉ (nouvel article 18/1 L.R&S)

44. Un nouvel article 18/1 L.R&S est ajouté:
Alinéa 1er : *« Dans l'intérêt de l'exercice de leurs missions visées aux articles1, 1° et 3° /1 et 11, § 1er, 1° à 3° et 5°, les services de renseignement et de sécurité peuvent mettre en œuvre des méthodes de recueil de données afin d'assurer la sécurité de leurs agents ou de l'exécution des missions. ».*

Conformément aux autres articles de la Loi Renseignement, le Comité suggère, **dans la version néerlandaise, de modifier comme suit la structure de début de l'alinéa com (REC-32)** : « *De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten bedoeld in de artikelen 7, 1° en 3° /1 en 11, § 1, 1° tot 3° en 5°, de (…) ».*

45. Le Comité constate que la disposition législative concernée prévoit la possibilité **d'utiliser toutes les méthodes de renseignement ordinaires, spécifiques et exceptionnelles pour des raisons de sécurité**, plus précisément afin d'assurer la sécurité des agents des services de renseignement et de sécurité ou la sécurité de l'exécution des missions. Or, nulle part dans l'exposé des motifs n'est fournie une justification ni une motivation expliquant pourquoi une méthode particulière est nécessaire à cette fin. Dans ce contexte, le Comité estime **que l'exposé des motifs doit justifier, pour chaque méthode de renseignement, pourquoi celle-ci est nécessaire à cette fin. Si une justification ne peut être trouvée que pour certaines méthodes bien précises, la disposition législative doit limiter son champ d'application à l'utilisation de ces méthodes (REC-33).**

46. Étant donné que la disposition en question ne reprend aucune méthode de renseignement mais définit uniquement le champ d'application d'un ensemble de méthodes, le Comité estime que le projet de loi **insère cette disposition au mauvais endroit dans la Loi Renseignement**. Actuellement, cette disposition figure dans la sous-section qui règle les méthodes ordinaires. Mais comme indiqué précédemment, cette disposition ne règle pas une méthode ordinaire. La justification de cet emplacement dans l'exposé des motifs n'est donc pas convaincante. Cette disposition législative devrait plutôt figurer dans la sous-section des dispositions générales, c'est-à-dire juste après l'actuel article 12 L.R&S.

De plus, en raison de l'insertion d'un nouvel article 18/1, l'actuel article 18/1 est **renuméroté** en article 18/2, et l'actuel article 18/2 est renuméroté en article 18/2/1. Le déplacement de l'article 18/1 proposé vers une disposition située juste après l'actuel article 12 L.R&S serait également conforme aux directives législatives du

Conseil d'État. Dans son guide de rédaction des textes législatifs et réglementaires, **le Conseil d'État déconseille vivement de renuméroter les articles d'un texte législatif à la suite de l'insertion d'un ou plusieurs articles entre des articles existants**.[46]

L'une des principales raisons à cela est que les références internes ou externes existantes aux éléments de texte renumérotés deviennent toutes erronées, ce qui peut donner lieu à des malentendus et à des erreurs (Voir J. Van Nieuwenhove, *Handboek wetgeving. Theorie en praktijk van het wetgevingsbedrijf*, Brugge, die Keure, 2025, p. 302-304). Le projet de loi prévoit en effet des modifications dans diverses références internes.

Tout cela nécessite de déplacer le projet d'article18/1 vers une disposition située après l'article 12 L.R&S dans la partie consacrée aux dispositions générales (REC-34).[47]

47. Alinéa 2 : *« Sans préjudice de l'article 13, § 4, les données à caractère personnel recueillies grâce à une méthode visée à l'alinéa 1er sont détruites, suivant les modalités fixées par le Roi, dès que le dirigeant du service concerné ou son délégué estime qu'il n'y a plus de danger pour la sécurité des agents ou de l'exécution des missions. ».*

Outre le déplacement de la disposition concernée, tel que décrit ci-dessus, le Comité recommande d'**ajouter les mots *« et de l'article 29 du Code pénal »* après les mots *« Sans préjudice de l'article 13, § 4 »* (REC-35)**. Ces derniers mots confirment l'obligation de signaler les informations relatives à des menaces, telle que décrite à l'article13, § 4 L.R&S dans le cadre de la méthode de renseignement ordinaire concernée. Le Comité approuve cette confirmation, mais rappelle que les informations en question peuvent également **contenir des informations relatives à des infractions pénales** qui peuvent donc présenter un intérêt pour le Ministère public.

48. Deuxièmement, le Comité recommande d'ajouter, à titre complémentaire, **une durée maximale de conservation d'un an** dans la disposition concernée **(REC-36)**.

(9) PROCÉDURE POUR LES MÉTHODES EXCEPTIONNELLES

Durée maximale à partir du début (projet d'article 18/10, § 1er, alinéa 2)

49. L'actuel article 18/10, § 1er, alinéa 2 stipule ce qui suit :
« Sauf disposition légale contraire, la période durant laquelle la méthode exceptionnelle de recueil de données peut être appliquée ne peut excéder deux mois, à compter de l'autorisation, sans préjudice de la possibilité de prolongation prévue au § 5. ».

Le projet de loi remplace cette disposition par ce qui suit :
« Sauf disposition légale contraire, la période durant laquelle la méthode exceptionnelle de recueil de données peut être appliquée qu'après l'autorisation, sans excéder deux mois, préjudice de la possibilité de prolongation prévue au § 5. ».

---

46 Conseil d'État, *Principes de technique législative. Guide de rédaction des textes législatifs et réglementaires,* 2008, p. 82-83 [disponible sur le site internet du Conseil d'État : https://www.raadvst-consetat.be/?page=technique_legislative&lang=fr).

47 Et, dans ce contexte, renuméroter la partie consacrée à l'IA en commençant par un nouvel article 12/2, qu'il serait également préférable de placer sous un titre distinct.

L'exposé des motifs motive cette modification comme suit : *« (…) cet article précise le début de la période maximale*[48] *pendant laquelle la méthode exceptionnelle de recueil de données peut être mise en œuvre. Il s'agit d'une analogie avec la procédure relative aux méthodes spécifiques, qui sise à rendre le cadre juridique plus cohérent et uniforme. Le délai maximal en vigueur ne fait l'objet d'aucune modification. »*.[49]

Le Comité **constate que, contrairement à ce qu'affirme l'exposé des motifs, l'article proposé supprime le début du délai maximal.**

La disposition proposée prévoit également qu'il peut y avoir des raisons de mettre en œuvre une méthode exceptionnelle sans autorisation. Dans l'article actuel, les termes « Sauf disposition légale contraire » font référence à la durée maximale de deux mois (à savoir que cette durée peut être exceptionnellement plus longue sur une base ad hoc, comme c'est le cas, par exemple, à l'article 18/13 L.R&S : le recours à un frontstore pour la collecte d'informations). Dans l'article proposé, ces mots font toutefois référence au fait de disposer d'une autorisation en tant que telle pour pouvoir utiliser une méthode exceptionnelle. La Loi Renseignement ne prévoit pas de telles exceptions. Un accord préalable est toujours requis, soit de la Commission BIM en réunion plénière, du président ou d'un membre de la Commission, ou encore du ministre de tutelle concerné.

Au vu de ces remarques, le Comité estime **que la modification concernée doit être supprimée dans son intégralité (REC-37).**

50. À l'article. 18/10, § 2, alinéa 1er L.R&S – qui énumère les mentions obligatoires dans une autorisation (ou un projet d'autorisation) *« la période durant laquelle la méthode exceptionnelle de recueil de données peut être appliquée à compter de l'autorisation du dirigeant du service »*, les mots *« à compter de l'autorisation du dirigeant du service »* sont supprimés au point 5°.

Compte tenu des remarques formulées ci-dessus, le Comité estime **que la modification concernée doit être supprimée dans son intégralité (REC-38)**.

(10) MISSION ET COMPÉTENCES D'ENTRAVE

51. Actuellement, la VSSE et le SGRS ont (uniquement) **la qualité de service de renseignement et de sécurité**. Le projet de loi propose d'**accorder à ces deux services le statut de service d'action**, non seulement à l'étranger, mais aussi sur le territoire belge. Cela signifie que, outre la détection et l'identification des menaces pour la sécurité nationale ainsi que la transmission des résultats d'enquête obtenus dans ce cadre à d'autres autorités susceptibles d'utiliser ces informations dans l'exercice de leurs compétences, le projet de loi charge ces deux services de prendre eux-mêmes des mesures offensives contre de telles menaces. Le Comité fait remarquer qu'il s'agit là d'un véritable **changement de paradigme** au sein de la communauté belge de la sécurité et demande donc que cette mesure ne soit pas mise en œuvre sans un débat démocratique approfondi.

Description d'une mission d'entrave (projet d'article 7, 5° et d'article 11, § 1er, 7° L.R&S)

52. La manière dont la nouvelle mission à ajouter est *décrite dans la loi* à l'article art. 7, 5° L.R&S (concernant la VSSE) – *" d'entraver les activités visées à l'article 7, 1° et 3°/1"* – et à article 11, § 1er, 7° L.R&S (concernant le SGRS) – *« d'entraver les facteurs, activités ou menaces visées sous 1° à 3° et 5° »* – pose problème à maints égards.

48 Passage souligné par le Comité.
49 Exposé des motifs, p. 61.

Ainsi, le Comité est d'avis que **le terme « entrave » est bien trop vague, surtout au regard des exigences posées par l'article 22 de la Constitution et l'article 8 CEDH**. La loi ne donne aucune description de ce terme, si bien qu'il n'y a guère de limites aux possibilités offertes aux services de renseignement. Le régime proposé est aussi **(partiellement) incompatible avec le principe de proportionnalité (par exemple l'article 8, alinéa 2 CEDH)**. Les termes utilisés ici vont également bien au-delà de la formulation employée dans l'exposé des motifs et dans l'accord de gouvernement 2025-2029.

Le Comité rappelle que l'article 7, 1° porte sur « toute activité qui menace ou pourrait menacer (…) ». En d'autres termes, il s'agit à la fois de menaces (« toute activité qui menace ») et – ceci est problématique dans le cadre d'une mission d'entrave – de menaces potentielles (« toute activité qui pourrait menacer »). Une telle description à l'article 7, 1° est tout à fait justifiée. En effet, la disposition concernée reprend la mission générale de renseignement. Il s'agit ici de collecter et d'analyser des informations dans le but de déterminer s'il existe une menace. Dans le contexte d'une mission d'entrave, un tel choix de mots aurait toutefois pour conséquence que la VSSE serait légalement autorisée à mener des actions d'entrave contre des activités susceptibles de constituer une menace, c'est-à-dire contre des activités dont il n'est pas certain qu'elles constituent (déjà) une menace. Non seulement c'est disproportionné, mais cela manque aussi cruellement d'efficacité. La sécurité nationale doit être protégée contre les menaces. Cela implique que la VSSE dispose d'informations concrètes et suffisantes sur une menace actuelle. Des actions d'entrave contre des activités qui ne peuvent pas encore être qualifiées de menace sont d'ailleurs choisies au hasard et, selon le Comité, n'ont pas leur place dans un État de droit démocratique.

La description à l'article 11, 7° est encore plus problématique étant donné que cette disposition s'écarte totalement du lien avec une menace. L'article 11, § 1er, 1°, première branche – qui reprend la mission générale de renseignement du SGRS, plus particulièrement le soutien en renseignement aux opérations militaires – a pour objet « 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 ». Comme à l'article 7, 1°, le Comité tient à souligner qu'une telle formulation est pleinement justifiée dans le cadre d'une mission de renseignement. Dans le contexte d'une mission d'entrave, une telle formulation aurait toutefois pour conséquence que le SGRS serait légalement autorisé à mener des actions d'entrave contre des activités qui ne présentent aucun lien avec une quelconque menace.

Comme indiqué précédemment, une telle formulation dans le projet de loi est surprenante, vu que tant de l'exposé des motifs lié au projet de loi que le passage concerné dans l'accord de gouvernement 2025-2029 ne parlent que de « menaces » et jamais de « menaces potentielles ». Ainsi dans **l'accord de gouvernement 2025-2029** figure ce qui suit : *« Une autorité résiliente est capable de faire face à des menaces telles que l'espionnage, l'ingérence, l'extrémisme et le terrorisme. Cela nécessite un service de renseignement fort, capable non seulement de détecter ces menaces à temps, mais aussi de les contrer. »*. Et ensuite : *« Grâce à une révision de la loi des services de renseignement et de sécurité, nous veillons à ce que la Sûreté de l'État, sous la supervision des organes de contrôle, soit en mesure de contrer efficacement les menaces (perturbation). »*.[50]

En outre, il n'est pas non plus justifié que le point 3° de l'article 11, § 1er soit repris dans la description légale de la mission d'entrave. La disposition concernée prévoit la mission relative au maintien de la sécurité militaire. Celle-ci consiste en (1) la sécurité du personnel, des installations, des armes et des systèmes d'armes, des

[50] Accord de gouvernement 2025-2029, p. 142.

munitions, des équipements, de plans, des écrits, des documents, des systèmes informatiques et de communications ou d'autres objets militaires [51], et (2) l'appui sécuritaire aux opérations militaires[52]. Le Règlement IF5 « Instruction sur la Sécurité Militaire » du 26 septembre 2023 du SGRS, entre autres, a toute son importance dans ce contexte. Ce règlement contient toutes les directives relatives à la sécurité militaire au sein du ministère de la Défense. La disposition en question n'est pas axée sur la menace, mais sur la protection ; elle ne peut donc pas servir de fondement à une mission d'entrave visant à lutter contre les menaces.

Le Comité fait également remarquer que les actions d'entrave empiètent presque par définition (profondément) sur la vie privée des citoyens (par exemple en suivant ostensiblement quelqu'un ou en faisant savoir à son entourage qu'il est la cible d'un service de renseignement). Elles peuvent être menées au grand jour avec la personne concernée, mais aussi en secret. Afin de prévenir tout abus potentiel, il est de jurisprudence constante de la Cour européenne des droits de l'homme que les mesures (en l'occurrence préventives et secrètes) prises pour faire face à des menaces pesant sur la sécurité nationale – pour être compatibles avec la CEDH et, en particulier, pour satisfaire aux exigences imposées aux restrictions de certains droits de l'homme (notamment l'article 8, alinéa 2 CEDH) ne sont autorisées qu'en cas de menace *grave et actuelle*[53] pour la sécurité nationale. [54]

Tant la Cour européenne des droits de l'homme que la Cour constitutionnelle considèrent qu'une ingérence dans la vie privée ne peut se fonder uniquement sur une base juridique « formelle ». La loi doit également être suffisamment accessible, prévisible et précise. **L'article 22 de la Constitution exigent que la loi elle-même définisse les conditions essentielles d'application et les garanties procédurales.**

53. Les raisons invoquées **requièrent tout d'abord une modification de la description de la mission d'entrave dans le sens suivant** :

- ***art. 7 : « d'entraver les menaces graves et actuelles telles que visées aux articles 7, 1° et 3°/1 »***
- ***art. 11, § 1er: « d'entraver les menaces graves et actuelles telles que visées sous 1° à 2°/1° et 5° »* (REC-39).**

Il convient par ailleurs d'inclure une définition suffisamment claire des actes susceptibles de relever de cette compétence.

Comme le Comité l'a déjà recommandé dans son *Analyse juridique des possibilités légales dont disposent les deux services de renseignement en matière d'entrave* (n° 2022.295 du 20 janvier 2023), une mission d'entrave doit, pour des raisons juridiques et techniques, être inscrite à l'article 7 L.R&S (à savoir l'énumération des missions de la VSSE) et à l'article 11 L.R&S (à savoir l'énumération des missions du SGRS). Le Comité tient néanmoins à rappeler que, compte tenu de l'article 22 de la Constitution, une activité d'entrave ne peut être menée que si elle est strictement nécessaire. De telles activités ne doivent pas revêtir un caractère routinier, mais doivent se limiter à des cas exceptionnels dans lesquels la nécessité requise a été démontrée de manière satisfaisante.

54. Sur le plan légistique, en particulier concernant **le lieu où se déroule la mission d'entrave (REC-40)**, le Comité rappelle que depuis 2016, le point 3° de l'article 7 L.R&S est une disposition sans objet compte tenu de la suppression de l'ancienne mission de protection de la VSSE. Il convient d'utiliser cette disposition pour la nouvelle mission d'entrave de la VSSE, notamment parce que le point 4° de l'article 7 L.R&S est une disposition

---

51 Art. 11, § 1er, 2°, première branche L.R&S.

52 Art. 11, § 1 er, 2°, première branche L.R&S, en comparaison de l'article 21, 1° AR Structure de la Défense (*a contrario*).

53 Par exemple l'arrêt n° 37138/14 du 12 janvier 2016 *Szabó et Vissy c. Hongarije* (2016), n° 75.

54 C'est pourquoi, par exemple, l'article 8bis de la Loi sur les étrangers exige que la condition de « menace grave et actuelle pour l'ordre public ou la sécurité nationale » soit remplie avant que certaines mesures puissent être prises.

résiduelle qui doit nécessairement figurer en dernier lieu dans une énumération légale des missions (art. 7, 4°: *« d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi »*).

La même remarque s'applique à la position de la mission d'entrave du SGRS à l'article 11, § 1er L.R&S. Le point 6° de l'article 11, 1er contient une disposition résiduelle similaire qui implique qu'elle doive figurer en dernier lieu dans une énumération légale des missions du SGRS.

55. Compte tenu des remarques susmentionnées, il convient également d'examiner **le projet de modification de l'article 9 L.R&S** (c'est-à-dire la compétence de réquisition de la VSSE à l'égard du SGRS) et **le projet de modification de l'article 11, § 3 L.R&S** (c'est-à-dire la compétence de réquisition du SGRS à l'égard de la VSSE) **(REC-41)**.

D'ailleurs, on comprend bien pourquoi ces deux dispositions font l'objet de modifications légistiques différentes.

Procédure d'entrave (projet d'article 19, alinéa 2, projet d'article 19/2 à 19/6 L.R&S)

56. Le projet de loi et l'exposé des motifs établissent **une distinction entre deux formes d'entrave.** D'une part, il y a l'entrave sous la forme d'une communication de renseignements (*cf*. art. 19 L.R&S) laquelle peut, le cas échéant, constituer une infraction pénale (soumis à l'actuel article 13/1 L.R&S selon les développements des modifications de l'article 19 L.R&S[55]). Dans l'exposé des motifs, on parle d' « entrave indirecte ».[56] Cette possibilité de transmettre des informations et des renseignements à d'autres autorités publiques, qui peuvent les utiliser dans le cadre de leurs compétences, a toujours existé. D'autre part, il y a l'entrave prenant la forme d'une action d'entrave (*cf*. projet d'article 19/2 à 19/6 L.R&S), laquelle peut, le cas échéant, constituer une infraction pénale (*cf*. projet d'article 19/3 L.R&S). Dans l'exposé des motifs, il est question d' « entrave directe ».[57]

57. Le problème est que le projet de loi, à l'exception de l'action d'entrave constituant une infraction pénale (ce qui mérite d'ailleurs d'être nuancé ; *infra*), confère la décision d'agir exclusivement au dirigeant du service de renseignement concerné, qui peut même déléguer cette compétence. Non seulement les services de renseignement se voient conférer la compétence d'exécuter une action d'entrave autorisée, mais aussi, en règle générale, celle de décider de sa mise en œuvre **sans aucun contrôle indépendant préalable** à cet égard. Dans ce contexte, le Comité attire l'attention sur l'une de ses recommandations adressées à la Commission de la Chambre chargée du suivi de la commission d'enquête parlementaire Attentats terroristes : *« […] le Comité est d'avis que dans un État démocratique et de droit, les activités d'entrave primaire de la VSSE (c'est-à-dire l'intervention d'initiative du service de renseignement dans le cadre d'une activité qu'il a lui-même qualifiée de menace) devraient être réglementées séparément dans une loi suffisamment claire, au sens formel du terme. L'idée sous-jacente est que différents organes doivent être chargés de détecter et d'enquêter sur les éventuelles menaces pour la sécurité nationale, d'évaluer la menace (in casu, il s'agit de déterminer si des individus, des groupes ou des événements constituent effectivement une menace pour la sécurité nationale) et de prendre les mesures nécessaires contre ces menaces. Au minimum, le pouvoir de décision d'intervention doit être entre les mains d'une instance autre que celle qui l'exécute. Une alternative consiste à établir un contrôle externe similaire au contrôle MRD. »*.[58]

---

55 Exposé des motifs, p. 75.

56 Auparavant, la VSSE désignait cela sous le nom d' « entrave secondaire » dans son règlement interne.

57 Auparavant, la VSSE désignait cela sous le nom d' « entrave primaire » dans son règlement interne.

58 COMITÉ R/I, Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité, n° 2022.294 (www.comiteri.be) et COMITÉ R/I, Analyse juridique des possibilités légales dont disposent les deux services de renseignement en matière d'entrave, n° 2022.295 (www.comiteri.be).

Un service de renseignement a la possibilité légale de qualifier une personne ou un groupe de menace pour la sécurité nationale. Ce sont toutefois les autorités politiques, judiciaires, administratives, policières ou diplomatiques, destinataires des informations fournies par les services de renseignement, qui ont le dernier mot et qui ont le pouvoir de prendre ou non des mesures de rétorsion dans le cadre de leurs missions et compétences légales. Le projet de loi confère désormais cette dernière compétence à la VSSE et au SGRS . Le Comité fait remarquer que divers organismes publics chargés de l'application de la loi ont à la fois le pouvoir de recueillir des informations et de prendre ensuite des mesures pour y remédier. Il y a toutefois quelques différences fondamentales. Tout d'abord, dans de tels cas, il existe un dossier administratif ou judiciaire contenant toutes les informations pertinentes, qui est, en règle générale, accessible à la personne concernée. En outre, les mesures que ces autorités peuvent prendre sont clairement définies par la loi et concrétisées par une décision motivée (ce qui n'est pas le cas de la possibilité d' « entraver » des menaces). Enfin, ces mesures de rétorsion peuvent faire l'objet d'un recours devant une juridiction indépendante et d'un contrôle par celle-ci. Ces garanties procédurales font défaut en cas d'entrave par un service de renseignement telle que développée dans le présent projet.

58. Le projet de loi ne prévoit l'autorisation préalable de la Commission BIM que dans le cas où une action d'entrave s'accompagne d'une infraction pénale : soit en vertu des dispositions de l'article13/1 L.R&S, soit en vertu de la disposition proposée à l'article 19/3 L.R&S. **Le Comité considère que le critère de distinction, à savoir le fait qu'une entrave constitue ou non une infraction pénale, ne suffit pas à garantir un contrôle externe indépendant et efficace d'une action d'entrave.**

En outre, **il existe un risque sérieux qu'un service de renseignement décide, dans le cadre d'un dossier, de mener une action d'entrave sans la faire passer par la Commission BIM, car il estime à tort qu'il ne s'agit pas d'une infraction pénale.** En d'autres termes, il y a un risque réel qu'un service de renseignement recoure à tort à la procédure visée au projet d'article 19/4 L.R&S, alors qu'il devrait recourir à celle visée au projet d'article 19/3 L.R&S. En 2010, le législateur a justement créé la Commission BIM, composée de trois magistrats (un juge d'instruction, un juge (pénal) et un magistrat de parquet) en raison de l'expertise de ceux-ci en matière de pouvoirs d'enquête et en matière pénale.

L'**exposé des motifs lui-même** contient des exemples d'actions d'entrave qui ne seraient pas constitutifs d'une infraction pénale : *« les agents (qui) placent une fausse caméra de manière très visible en face du domicile de la personne dont leurs services de renseignement veulent entraver l'activité menaçante »* et *« une filature ostensible de la personne en présence de ses contacts pour griller leurs relations »*.[59] Ces deux actions peuvent relever de l'infraction de harcèlement (art. 442*bis* CP-1867; art. 237 CP-2024). Cette infraction se définit comme « le fait de troubler gravement et intentionnellement la tranquillité d'une personne, même s'il s'agit d'un acte ponctuel ou d'un acte isolé, alors que l'on savait ou aurait dû savoir que ce comportement affecterait gravement la tranquillité de la personne visée ». Cet exemple, tiré de l'exposé des motifs, illustre à lui seul l'expertise requise en matière de qualification pénale.

Enfin, le Comité rappelle un passage dans l'exposé des motifs de la Loi du 14 juillet 2022 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (*M.B.* 5 août 2022). Plus précisément, il est indiqué ce qui suit : *« Les mots "les faits susceptibles d'être qualifiés infraction(s) »* – c'est-à-dire la mention obligatoire dans la demande du service de renseignement à la Commission BIM en vue de la commission d'infractions dans le cadre d'une mission de renseignement (*cf*. article 13/1, § 3, alinéa 4, 1° L.R&S) – *« sont utilisés afin que la demande contienne les faits précis qui sont planifiés. Par contre, la qualification elle-même, qui n'entre pas dans les compétences d'un service de renseignement, est laissée à l'appréciation de la*

[59] Exposé des motifs, p. 78.

Commission. ».[60] Il n'existe aucune justification objective permettant de considérer que la Commission BIM devrait être compétente pour la qualification pénale des activités envisagées par les services de renseignement dans le cadre de la collecte d'informations, alors qu'elle ne le serait pas pour l'exécution d'actions d'entrave. De plus, cette garantie procédurale revêt une importance encore plus grande dans le cadre de ces dernières activités, car leur impact sur les individus est plus important. **La décision selon laquelle certaines activités envisagées par les services de renseignement ne constituent *pas* une infraction pénale est d'ailleurs tout aussi importante et nécessite au moins autant d'expertise que la définition de la ou des infractions pénales précises qu'une action d'entrave entraînerait.** À l'estime du Comité, ce fait suffit à lui seul à justifier que toute action d'entrave envisagée soit soumise à la Commission BIM.

59. Dans le projet de loi, un service de renseignement ne se contente donc pas de décider lui-même s'il considère une personne ou un groupe comme une menace pour la sécurité nationale ; il décide également lui-même s'il convient de mener une action d'entrave à l'encontre d'une telle personne ou d'un tel groupe, et il met en œuvre cette action d'entrave de manière autonome (sans contrôle externe préalable). Compte tenu de cette situation, **le Comité émet un avis défavorable sur l'ensemble de la procédure d'entrave proposée dans le projet de loi et insiste pour que celle-ci soit entièrement revue (REC-42)**.

Le Comité rappelle l'accord de gouvernement 2025-2029 qui indique que *« (…) sous la supervision des organes de contrôle (la Sûreté de l'État), soit en mesure de contrer efficacement les menaces (perturbation). ».*[61] **L'exigence d'un contrôle par les organes de contrôle n'est en aucun cas suffisamment prise en compte dans le présent projet de loi.** Le Comité souligne qu'un contrôle a posteriori – tel que le contrôle effectué par le Comité conformément à la Loi Contrôle du 18 juillet 1991, mais aussi les notifications mensuelles au Comité prévues au projet d'article 19/5, § 7 L.R&S – donc *après* que l'action d'entrave a été menée – ne satisfont pas à l'exigence d'un contrôle préalable, indépendant et contraignant. Affirmer que le Comité peut toujours effectuer un contrôle conformément à la Loi Contrôle ne remédie donc pas à l'absence légale d'un contrôle a priori de toutes les actions d'entrave. Affirmer, comme c'est le cas dans le projet d'article 19/5, § 8 L.R&S que *« [l]a Commission et le Comité permanent R peuvent à tout moment contrôler la légalité de l'entrave visée aux articles 19/3 et 19/4 »* n'est pas non plus suffisant. Affirmer que les organes de contrôle peuvent « à tout moment » effectuer un contrôle ne change en effet rien au fait qu'aucun accord n'est demandé au préalable à un organisme de contrôle indépendant .

60. Afin de remédier aux problèmes décrits ci-dessus, toutes les actions d'entrave doivent être soumises au préalable à l'autorisation d'une autorité externe. La procédure existante relative aux méthodes d'enquête exceptionnelles, selon laquelle toute méthode exceptionnelle prévue doit être soumise au préalable à l'autorisation de la Commission BIM (ce que l'on appelle un avis contraignant/conforme) et selon laquelle un contrôle juridictionnel est exercé en deuxième instance par le Comité, peut, le cas échéant, servir de modèle. Cette procédure a prouvé son utilité ainsi que sa solidité sur le plan pratique et juridique.

61. Une modification doit également être apportée dans l'intérêt des agents d'exécution des services de renseignement. Si un service de renseignement décide qu'une action d'entrave ne constitue pas une infraction, alors que les autorités judiciaires en jugent autrement par la suite, cela signifie que les agents d'exécution de ce service de renseignement commettent une infraction sans que celle-ci soit couverte par la loi. Dans un tel cas, les agents d'exécution – mais aussi le dirigeant du service qui a donné son autorisation – s'exposent à des poursuites pénales, qui peuvent, le cas échéant, être engagées par une partie civile (par exemple par le target qui a fait l'objet de l'entrave).

---

60 *Doc. parl.* Chambre 2021-2022, n° 55-2706/001, 25.

61 Accord de gouvernement 2025-2029, p. 142.

62. Par ailleurs, le Comité estime **que la décision du dirigeant du service, telle que décrite au projet d'article 19/3, § 2 et qui comporte diverses mentions obligatoires, doit s'appliquer à toutes les formes d'entrave, que cette entrave se produise par le biais d'une transmission d'informations (*cf*. projet de deuxième alinéa de l'article 19) ou par le biais d'une action d'entrave, et que cette entrave constitue ou non une infraction pénale.** L'entrave constitue une mesure trop extrême pour que le législateur n'ait pas à intervenir sur les exigences de forme obligatoires d'une telle décision.

Entrave par le SGRS (les Forces armées) sur le territoire belge

63. Le Comité rappelle que le SGRS fait partie des Forces armées. En temps de paix, dans le cadre de la mise en œuvre concrète sur le terrain, la police est généralement chargée de la sûreté intérieure, tandis que les forces armées sont compétentes en matière de sûreté extérieure. Sous certaines conditions légales et réglementaires, les forces armées peuvent également être mobilisées sur le territoire belge en temps de paix. **La compétence octroyée au SGRS de mener des actions d'entrave sur le territoire belge revient à faire intervenir les forces armées sur le territoire belge d'une autre manière dans le cadre d'une simple mission de renseignement.** Le Comité constate que cet aspect n'a pas été abordé dans l'exposé des motifs. **Il recommande d'en faire un sujet de débat et, le cas échéant, d'encadrer une telle activité par des formes supplémentaires de prise de décision politique (REC-43).**

Entrave par le SGRS dans le cyberespace

64. En confiant cette mission d'entrave au SGRS, ce service de renseignement se voit également attribuer le pouvoir de mener des actions d'entrave dans le cyberespace. En vertu de l'Arrêté royal fixant la structure générale du ministère de la Défense, il existe au sein du SGRS un ***Commandement cyber*** (Cyber Command) qui opère dans le cyberespace et qui remplit des missions définies à l'article 11 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.[62] Il convient de distinguer (juridiquement) le Commandement cyber de la ***Force cyber*** (Cyber Force). Il s'agit de l'une des cinq forces (de combat) au sein des Forces armées belges.[63]

Le projet de loi prévoit **que le Commandement cyber n'aura plus de compétences uniquement dans le domaine du cyber-renseignement et de la cybersécurité**, mais se voit également attribuer la compétence de mener des **cyberattaques** qui ne se limitent pas à une simple contre-attaque mais qui s'étendent aussi à des actions d'entrave dans le cyberespace. Dans ce contexte, et compte tenu de la distinction entre le Commandement cyber et la Force cyber, la question se pose de savoir quelles cyberactivités offensives pourraient encore être légalement attribuées à la Force cyber, autres que celles qui relèvent du champ d'application des actions d'entrave visées dans le projet d'article 19/2 à 19/6 L.R&S. **Le Comité recommande de préciser ce point dans l'exposé des motifs (REC-44).**

En outre, le Comité recommande d'**inclure dans la loi une définition de la notion de « cyberattaque » (REC-45**), ainsi que de préciser si et dans quelle mesure cette notion coïncide avec une action d'entrave dans le cyberespace.

---

62 *Cf*. art. 42, alinéa 1er A.R. du 30 juin 2025 fixant la structure générale du Ministère de la Défense et les attributions de certaines autorités (*M.B.* 15 juillet 2025 ; ci-après : AR Structure Défense).

63 En plus des composantes Terre, Air, Marine et Médicale (*cf*. art. 1er, alinéa 1er, 5° AR Structure Défense).

Actions d'entrave interdites

65. Le projet de loi prévoit l'interdiction de la violence (projet d'article 19/2, alinéa 2 L.R&S) et l'interdiction d'entraver une enquête pénale (projet de modification de l'article 13/5 L.R&S) au cours d'une action d'entrave. Le Comité souligne l'importance de ces deux dispositions d'interdiction.

Le Comité tient toutefois à souligner la nécessité de compléter la définition de l'**interdiction de la violence**. La formulation actuelle est la suivante : *« En aucun cas l'entrave ne peut porter délibérément atteinte à l'intégrité physique des personnes. »*. Le Comité fait remarquer que seules **les atteintes « *délibérées* » à l'intégrité physique** sont explicitement interdites. Les atteintes à l'intégrité physique **résultant d'un « *manque de précaution et de prudence* », qu'il soit grave ou non**, ne relèvent pas du champ d'application de cette interdiction. Une action d'entrave qui porte ainsi atteinte à l'intégrité physique d'une personne en raison d'une négligence (grave) ou d'un manque (grave) de prudence de la part de la VSSE ou du SGRS ou de la part d'un tiers agissant pour le compte d'un service de renseignement, ne relève pas de cette disposition. Ainsi, dans sa forme actuelle, le projet permet par exemple à la VSSE/au SGRS de faire courir au sein d'un groupe la rumeur (fausse) selon laquelle la personne X serait un informateur. Outre le fait que le Comité estime que de telles « actions » dépassent largement les limites de ce qui est admissible, cela peut donner lieu à des représailles de la part de tiers. Une interdiction formulée de manière plus large incitera les services à prendre conscience que toute action d'entrave exige une préparation et une exécution rigoureuses. Dans un tel cas, l'État fédéral risque d'être tenu civilement responsable d'un acte commis par un service de renseignement. **Le Comité demande, dans le projet d'article 19/2 et 19/6 § 1er soit d'ajouter les mots « par manque de précaution et de prudence », soit de supprimer le mot « délibérément » (REC-46).**

66. De plus, dans le projet de loi, le mot « délibérément » est aussi ajouté aux **articles 13/1, § 4, 13/1/1, § 3 et 18/10, § 3/1, dernier alinéa**. Le Comité estime **que ces dispositions doivent elles aussi faire l'objet d'une adaptation similaire (REC-47).**

67. Le Comité est d'avis **que l'interdiction de la violence doit également s'appliquer explicitement à l'entrave via la transmission d'informations sur la base de l'article 19, alinéa 2 L.R&S (communication au target même ou à des tiers qui peuvent effectuer l'entrave) et de l'article 19, alinéa 3 adapté (communication à la presse et au public) (REC-48)**. Une disposition légale dans le sens de *« [l'] entrave ne doit en aucun cas, que ce soit délibérément ou par manque de précaution ou de prudence, porter atteinte à l'intégrité physique des personnes. »* doit attirer l'attention de la VSSE et du SGRS et les rendre responsables du fait que la divulgation d'informations sensibles à certains tiers, voire au grand public, n'est pas toujours anodine et peut inciter des personnes à commettre des actes de violence. Le Comité ne partage pas l'avis selon lequel les services de renseignement ne peuvent en aucun cas être tenus responsables des actes commis par des tiers utilisant ces informations des services de renseignement, surtout lorsque ces informations sont rendues publiques par les services de renseignement avec une finalité d'entrave.

68. Le Comité estime, en outre, que ces deux dispositions d'interdiction ne suffisent pas. Le Comité reconnaît que certaines évolutions sociales nécessitent l'attribution de compétences supplémentaires à la VSSE et au SGRS. Cela doit se faire parallèlement à la mise en place de certaines limites par le législateur. **Aussi, selon le Comité, il convient également de prévoir une interdiction légale explicite d'exercer des activités policières sous couvert d'actions d'entrave (REC-49).**

Ni l'accord de gouvernement, ni l'exposé des motifs ne laissent entrevoir la moindre volonté de transformer la VSSE et le SGRS en un service de police. Toutefois, en l'absence de description concrète d'une action d'entrave – hormis quelques exemples casuistiques figurant dans l'exposé des motifs et une référence au dictionnaire (Le Robert et Van Dale) – il n'existe aucune garantie juridique que les actions d'entrave décrites ci-dessus soient exclues à l'avenir.

69. La Constitution et les traités internationaux garantissent la jouissance d'un certain nombre de droits fondamentaux. Pour certains d'entre eux, une limitation par l'État est possible moyennant une intervention législative et le respect des critères de nécessité et de proportionnalité. Pour d'autres, aucune dérogation n'est admise (par exemple l'interdiction de la torture et des traitements inhumains ou dégradants). Cet aspect n'est pas abordé dans le projet de loi, alors que, sans pour autant constituer une infraction, une action d'entrave peut avoir pour effet de porter atteinte à ces droits fondamentaux. À titre d'exemple, en ce qui concerne le droit à la vie ou l'interdiction de traitements inhumains et dégradants, on peut imaginer le cas d'une communication de données à caractère personnel d'un individu représentant une menace si ces informations sont communiquées à un service partenaire susceptible de prendre des mesures à l'encontre de cette personne.
Le Comité est d'avis que ces cas de figures, possibles et non interdits dans le projet actuel, doivent faire l'objet d'un encadrement particulier dans la loi, en prévoyant une liste fermée d'actions d'entrave interdites (ou inversement : autorisées) et un régime d'autorisation et de contrôle approprié pour les entraves ayant un impact négatif sur un droit fondamental garanti par la Constitution ou un traité international. (REC-50). À titre d'exemple, le droit canadien prévoit une procédure d'autorisation par une autorité indépendante pour les entraves qui pourraient porter atteinte aux droits fondamentaux d'un individu ou qui sont contraires au droit canadien.[64]

Entrave contre des mandataires politiques

70. Dans son Rapport d'activités 2021, le Comité écrivait : *« Lors de débats (parlementaires), une question est posée à maintes reprises, à savoir si et dans quelle mesure les services de renseignement belges suivent (ou sont autorisés à suivre) des mandataires politiques, et quelles règles doivent être observées à cet égard. Depuis début janvier 2018, une note de service classifiée 'CONFIDENTIEL' est d'application au sein de la VSSE. Conformément à cette note, actualisée en juin 2020 [65], le service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports ponctuels sur des mandataires politiques qui contribueraient à l'apparition d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble des documents dans lesquels des mandataires politiques sont mentionnés.60 Le ministre de la Justice avait marqué son accord sur le « principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991 ».[66] Étant donné qu'il n'est mentionné nulle part ce que le Comité permanent R est censé faire des informations précitées, il a pris l'initiative de développer une méthodologie autour de cette problématique et de son rôle de contrôle. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020. ».*[67]
Les mandataires politiques visés sont les ministres des différents gouvernements, le Commissaire belge siégeant à la Commission européenne et les membres des différents parlements et assemblées, y compris les membres belges du Parlement européen. Les autres élus ou mandataires désignés ne sont pas concernés (par exemple les échevins au niveau communal ou les gouverneurs au niveau provincial).[68]

Et indique en outre ce qui suit : *« Dans le cadre de son fonctionnement opérationnel, la VSSE ne réserve pas aux mandataires politiques un traitement différent de celui accordé aux autres catégories professionnelles. S'il existe des raisons d'examiner de plus près l'éventuelle implication d'un mandataire politique dans la survenue d'une menace, il convient de le faire. Sauf bien sûr dans les cas où le mandataire politique est impliqué en tant que*

64 Section 12.1 du Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23).

65 Contrairement aux notes de service précédentes, cette note de service actulisée n'est pas classifiée.

66 *Cf.* Lettre du ministre de la Justice du 26 juillet 2018 adressée au Comité R concernant 'Le recueil d'informations par un service de renseignement concernant une personne exerçant un mandat politique', mentionné dans : COMITÉ R, Rapport d'activités 2021, p. 31, note infrapaginale 61.

67 COMITÉ R/I, *Rapport d'activités 2021*, p. 30-32.

68 Note de service n° 20-28, p. 2, mention dans : COMITÉ R/I, Analyse juridique des possibilités légales dont disposent les deux services de renseignement en matière d'entrave, enquête de contrôle n° 2022.295, du 20 janvier 2023, p. 2.

victime dans la survenue d'une menace. Toutefois, lorsque des mandataires politiques sont concernés, un certain nombre de mécanismes doivent être appliqués afin d'éviter tout abus de position de la part du service. Parmi ces mécanismes figure notamment le devoir d'information aux ministres compétents dès qu'il y a présomption d'implication d'un mandataire politique dans la survenue d'une menace. ».[69]

Dans son analyse juridique des possibilités légales dont disposent les deux services de renseignement en matière d'entrave – également mentionné dans l'exposé des motifs – le Comité affirme qu' *« **[i]l ressort clairement** des notes de service n° 20-28 et n° 20-29 que la VSSE s'estime compétente pour prendre des mesures perturbatrices à l'encontre des activités des **parlementaires fédéraux et régionaux et des ministres qualifiés de problématiques**, et manifestement tant pour des disruptions secondaires (c'est-à-dire informer et conseiller les autorités compétentes) **que pour des disruptions primaires (c'est-à-dire prendre elle-même des mesures d'exécution).** ».*[70]

Le présent projet de loi ne prévoit aucune mesure d'entrave à l'encontre des mandataires politiques, qui, selon l'évaluation du service de renseignement concerné, représentent une menace pour la sécurité nationale. **Le Comité recommande d'en faire un sujet de débat et, le cas échéant, de prévoir dans la loi des conditions procédurales supplémentaires à cet égard (REC-51)**.

Entrave par la transmission d'informations versus entrave par une action d'entrave

71. En ce qui concerne une entrave par la transmission d'informations (projet d'article 19, alinéa 2 L.R&S), l'exposé des motifs donne notamment l'exemple suivant :
*« Le message peut être explicite, comme c'est le cas du mot dans la boîte aux lettres ou implicite. La communication doit se comprendre dans un sens large ; elle peut être écrite, verbale ou non-verbale. La communication non-verbale d'informations à la personne surveillée par les services de renseignement en vue d'une entrave pourrait ainsi résulter indirectement d'une méthode de recueil, par exemple lors d'une inspection clandestine dans le domicile de la personne pour inventorier le matériel qui serait en sa possession, **les agents de renseignement laissent volontairement des traces de leur passage, faisant ainsi passer le message « nous savons ce que vous préparez** .».*[71]

Le Comité considère qu'une telle **« communication non verbale »** [72] ne relève pas du champ d'application du projet d'article 19, alinéa 2 L.R&S (à savoir la transmission d'informations) mais du projet d'article 19/2 à 19/6 L.R&S (à savoir l'action d'entrave). Il ne s'agit en aucun cas de la transmission et de la communication d'informations à un organisme (public) tiers qui aurait ainsi la possibilité de prendre des mesures à l'encontre de la personne concernée sur la base de ces informations, mais bien de la mise en œuvre de mesures de rétorsion par ses propres moyens. En d'autres termes, il s'agit d'une intervention en toute autonomie visant directement à entraver une menace.

Cet exemple montre que le critère de distinction consistant à « commettre des infractions » n'est pas applicable dans le cadre d'actions d'entrave (projet d'articles 19/2 à 19/6 L.R&S), mais **que la distinction entre l'entrave via la transmission d'informations (projet d'article 19, alinéa 2 L.R&S) et l'entrave via une action d'entrave est souvent floue et s'avérera inopérante dans la pratique.**

---

69 Note de service de la VSSE n° 20-28, p.. 4-5, mention dans : COMITÉ R/I, Enquête de contrôle n°2022.295, p. 21.
70 COMITÉ R/I, Enquête de contrôle n°2022.295, p. 21.
71 Exposé des motifs, p. 73.
72 *Ibid*.

72. Le projet d'article 19/5, § 9 prévoit que *« [l]es articles 19/3 et 19/4 ne sont pas applicables à l'entrave effectuée en exécution de l'article 19 ou en exécution d'autres missions qui sont confiées aux services de renseignement et de sécurité par ou en vertu de la loi. ».* L'exposé des motifs donne un autre exemple de ce type : *« La réalisation d'enquêtes de sécurité dans le contexte de la délivrance des habilitations de sécurité telle que visées aux articles 7, 2° et 11, 4° (…) »* [73] ainsi que d'autres types de screenings de sécurité (par exemple les vérifications de sécurité).[74]

Pour les raisons exposées ci-dessus, le Comité considère **qu'une entrave par la transmission d'informations (*cf.* le projet d'article 19, alinéa 2 L.R&S), une entrave par une action d'entrave ne constituant pas une infraction pénale et une entrave par une action d'entrave constituant une infraction pénale doivent être soumises à la même procédure, avec les mêmes conditions de fond et de forme.**

73. Enfin, il est indiqué dans l'exposé des motifs que *« [d]e telles entraves* – c'est-à-dire celle qui sont visées par la transmission d'informations *cf.* article 19 L.R&S (nda) – *« ne seront entreprises qu'après une analyse approfondie des risques qui démontre le caractère proportionnel de l'entrave : équilibre entre le but recherché de contrer une activité menaçante au regard de sa gravité et les conséquences. ».* Le Comité salue l'exigence d'**une analyse des risques**. Il estime toutefois **que son élaboration doit être rendue obligatoire par la loi, et que l'exposé des motifs doit mentionner et décrire les différents aspects devant au moins être abordés dans une telle analyse des risques, notamment la nature des risques à contrôler (par exemple, les risques opérationnels, les risques juridiques, les risques liés à la sécurité, etc.). L'analyse des risques doit être formalisée et doit faire partie du dossier qui est mis à la disposition de ou des instance(s) de contrôle (REC-52).**

Subsidiarité et proportionnalité

74. Toute activité d'entrave doit logiquement **respecter** les principes de proportionnalité et de subsidiarité. Le projet d'article 19/3, § 2, 6° L.R&S le confirme, en exigeant que « la subsidiarité et la proportionnalité telles que visées à l'article 19/5 » doivent être décrites dans la décision du dirigeant du service. Le projet d'article 19/5, § 1er prévoit ce qui suit : *« La décision du dirigeant du service visée aux articles19/3 et 19/4 est dûment motivée quant à la proportionnalité et à la subsidiarité de l'entrave »*. Cette dernière disposition stipule clairement que ces deux principes doivent donc être respectés lors de toute action d'entrave, qu'elle constitue ou non une infraction pénale.

Le Comité attire l'attention sur le fait que le projet d'article 19/2 ne contient qu'une définition juridique de l'exigence de proportionnalité. Le Comité est d'avis **que le principe de subsidiarité soit également être défini juridiquement dans la disposition en question (REC-53)**.[75] Selon le Comité, la subsidiarité doit ici porter à la fois sur *la nécessité de lutter contre la menace pour la sécurité nationale en question* et sur le fait que *les mesures autres qu'une action d'entrave semblent insuffisantes*. À cet égard, l'utilisation des termes « semblent être » indique non pas qu'il faille effectivement essayer d'autres mesures au préalable, mais que c'est ce qui ressort de la motivation et du projet de décision.

Informations concrètes

75. Nulle part dans le projet de loi il n'est exigé que la VSSE et le SGRS ne puissent entraver des menaces que s'ils disposent d'informations concrètes sur l'existence d'une telle menace. **Le Comité estime que des rumeurs**

---

73 Exposé des motifs, p. 7.

74 Exposé des motifs, p. 79.

75 En ce qui concerne l'application des méthodes spécifiques et exceptionnelles, la Loi Renseignement contient également une définition juridique tant de l'exigence de proportionnalité que de l'exigence de subsidiarité.

ou de vagues soupçons ne suffisent pas pour justifier des mesures aussi radicales. C'est d'autant plus vrai lorsque des mesures qui ont des conséquences négatives pour des personnes physiques ou morales sont prises: les principes généraux de bonne administration exigent qu'une autorité publique dispose d'informations concrètes suffisantes pour justifier une mesure. Affirmer, le cas échéant, que la VSSE et le SGRS sont des services de renseignement qui ne collectent pas de preuves mais uniquement des renseignement est totalement infondé si ces informations sont utilisées pour justifier des mesures. **Le Comité demande de le confirmer dans l'exposé des motifs (REC-54).**

Procédure de régularisation

76. Le projet d'article 19/5, § 5 L.R&S prévoit ce qui suit : *« Si, **en raison de circonstances imprévisibles**, des faits susceptibles d'être constitutifs d'infraction(s) ont été commis dans le cadre de l'entrave visée aux articles 7, 5° et 11, 7° pour lesquels la procédure prévue à l'article19/3 n'a pas pu être suivie, le dirigeant du service en informe la Commission par écrit dans les plus brefs délais et au plus tard le jour ouvrable qui suit sa prise de connaissance de la commission des faits susceptibles d'être constitutifs infraction(s). Si la Commission estime que les faits ont été commis dans le cadre de l'entrave visée aux articles 7, 5° et 11, 7°, ils ne sont pas constitutifs d'infractions. ».*

77. Le Comité constate que dans la procédure actuelle, les articles 13/1 et 13/1/1 L.R&S – à savoir la commission d'infraction dans le cadre de la collecte d'informations – prévoient le recours à la cause d'excuse absolutoire, et que, dans la procédure proposée à **l'article 19/2 et suiv. L.R&S** – à savoir la commission d'infraction dans le cadre d'une action d'entrave –, le recours à une cause de justification. **Le Comité demande soit d'appliquer dans les deux cas une cause d'excuse absolutoire, soit de justifier plus en détail cette distinction dans l'exposé des motifs (REC-55).**

En outre, le Comité constate que l'exposé des motifs semble indiquer que des infractions peuvent également être commises dans le cadre d'une action d'entrave conformément **à l'article 19, alinéa 2,** à savoir l'entrave par la communication à un target, entre autres. **Le Comité demande de préciser cet aspect (REC-56).** Vu que l'article 19 L.&S ne contient pas de procédure pour la commission d'infractions, il conviendrait, dans un tel cas, de recourir à la procédure prévue à l'article 13/1 ou 13/1/1 L.R&S (où le législateur a prévu une cause d'excuse absolutoire). Si cette interprétation est correcte, le Comité demande **soit d'appliquer, comme ci-dessus, un instrument pénal identique, soit de justifier cette distinction dans l'exposé des motifs.**

78. Le Comité attire l'attention sur le fait que la procédure de régularisation en question – qui repose sur la procédure de régularisation décrite à l'article 13/1, § 7 L.R&S – ne peut s'appliquer qu'**en cas de circonstances imprévues**. Cette procédure ne peut donc pas s'appliquer lorsqu'un service de renseignement a entrepris une action d'entrave 19/4 L.R&S (seulement la décision du dirigeant du service, pas d'obligation d'accord préalable de la Commission BIM), là où il s'avère par la suite que cela aurait dû figurer à l'article 19/3 L.R&S (avec l'obligation de l'accord préalable de la Commission BIM). Dans ce cas, il ne s'agit en effet pas de circonstances imprévues : **les activités comprises dans l'actions d'entrave seront connues à l'avance et sont donc toujours prévisibles.** C'est également pour cette raison que le Comité préconise la mise en place d'une procédure uniforme, que l'action d'entrave constitue ou non une infraction pénale.

79. Le Comité constate que dans la procédure de régularisation actuelle, à 13/1, § 7 L.R&S, la Commission BIM doit aussi contrôler l'imprévisibilité : *« L'agent qui a commis ces faits bénéficie de l'exemption de peine si la Commission estime qu'ils étaient imprévisibles et strictement nécessaires pour assurer sa propre sécurité ou celle de tiers. »*. Ceci n'est pas défini dans la procédure de régularisation figurant dans le projet d'article 19/5, § 5 : *« Si la Commission estime que les faits ont été commis dans le cadre de l'entrave visée aux articles 7, 5° et 11, 7°, ils ne sont pas constitutifs d'infractions. »*. Le Comité juge fondamental un contrôle de l'imprévisibilité des faits punissables par la Commission BIM. Plus encore dans le cadre d'une action d'entrave, étant donné que la

décision de la Commission BIM supprime l'illicéité des infractions, alors que, dans le cadre de l'article 13/1, § 7, l'illicéité subsiste mais qu'en principe, aucune sanction pénale ne peut être requise ou prononcée. **Le Comité considère que, dans le cadre de la procédure de régularisation aussi, la Commission BIM doit contrôler le caractère imprévisible des actions d'entrave. Il estime que cela doit être ajouté dans la loi (REC-57).**

Concours avec une enquête pénale

80. Il ressort du projet d'article 19/3, § 2, alinéa 2 L.R&S que la mention de « concours » – d'une action d'entrave – « avec une information ou une instruction judiciaire » (§ 2, alinéa 1er, 7°) comme mention dans la décision du dirigeant du service de renseignement n'est pas obligatoire sous peine de nullité. Le Comité rappelle qu'une menace pour la sécurité nationale constituera aussi souvent une infraction pénale, notamment en ce qui concerne les menaces relevant de la compétence de la VSSE (voir par exemple : la récente mise à jour de la définition de l'infraction d'espionnage, la récente incrimination de l'infraction d'ingérence, la portée étendue de l'infraction de terrorisme). Dans cette optique, le Comité estime **que la mention concernée doit être imposée sous peine d'illégalité (REC-58)**.

Contrôle par la Commission BIM et le Comité R/I

81. Outre les problèmes exposés ailleurs, le projet d'article 19/5, § 8, qui prévoit un contrôle de légalité par la Commission BIM et le Comité sur les entraves visées aux projets d'articles 19/3 et 19/4, souffre d'un manque de précision quant à la manière dont ces deux organes doivent exercer leur contrôle. Dans le cadre du contrôle des méthodes particulières de renseignement, l'ordre dans lequel les deux instances interviennent est décrit, et celui-ci correspond globalement respectivement à un contrôle préalable et en temps réel et à un contrôle a posteriori. Dans ce contexte, le contrôle exercé par la Commission BIM constitue un contrôle administratif de première ligne, tandis que le contrôle exercé par le Comité R/I est un contrôle de deuxième ligne de nature juridictionnelle. De même, dans le cadre de certaines mesures de protection et de soutien (par exemple en cas de commission d'infractions), il est prévu que la Commission BIM prenne une décision, contre laquelle le service de renseignement peut, le cas échéant, introduire un recours auprès du Comité.
La présente réglementation ne prévoit aucun mécanisme, ce qui comporte le risque d'un conflit de compétences entre les deux instances. **Le Comité recommande donc, dans le cadre de la révision plus large de cette matière qu'il préconise, de définir les modalités de contrôle respectives de la Commission BIM et du Comité, et de préciser comment ces formes de contrôle s'articulent entre elles (REC-59).**

Remarques linguistiques au projet d'article 19, alinéa 2 L.R&S

82. Projet d'article 19, alinéa 2 L.R&S : *« Les services de renseignement et de sécurité peuvent communiquer des informations et données à caractère personnel à des personnes ou instances qui font l'objet d'une entrave visée aux articles 7, 5° et 11, 7°. ».*

Le Comité propose de **(REC-60)**:
- remplacer, dans la version néerlandaise, la notion de « *onderwerp* » par la notion de « *voorwerp* »
- remplacer la notion d' « information » – qui, au sein de la communauté du renseignement, fait référence aux données brutes – par la notion de « renseignement » – qui fait référence à une information traitée.

83. Dans la version en langue française, tant le projet d'article 19/3, § 1er, alinéa 1er que le projet d'article 19/4, § 1er , alinéa 1er indiquent de la même manière : *« Sous réserve de l'article 19 et d'autres dispositions spécifiques aux missions (…) »*. Le Comité constate que cette phrase est traduite différemment dans les deux articles. Afin

d'éviter toute confusion, le Comité recommande de prévoir également une traduction exacte dans la version néerlandaise **(REC-61)**.

84. Tant le projet d'article 19/3, § 1er, alinéa 2 que le projet d'article 19/4, § 1er, alinéa 2 contiennent la notion « faits passibles de SAC » **(REC-62)**. Pour ce qui est de cette modification, le Comité renvoie à l'examen des modifications proposées à l'article 13/1 L.R&S.

(11) RÉQUISITION DU CONCOURS DE TIERS (projet d'article 18/10, § 3/1-§ 3/4 et article 19/6 L.R&S)

85. Le projet de loi crée un pouvoir de réquisition, sanctionné pénalement, visant à obtenir le concours de tiers dans le cadre de la mise en œuvre de méthodes de renseignement exceptionnelles (projet d'article 18/10, § 3/1 - § 3/4 L.R&S) et de missions d'entrave (projet d'article 19/6, § 1er - § 6 L.R&S).

En vertu de ces deux dispositions, *quiconque*, en temps de paix, sur le territoire national ou à l'étranger, quelle que soit sa qualité (par exemple, agents de police, membres de l'administration publique) ou son éventuel statut protégé (par exemple, mineurs, avocats, journalistes, médecins), peut être contraint, sous peine de sanctions pénales, de collaborer avec la VSSE et le SGRS. Ces deux dispositions ne comportent pas non plus de description concrète, et encore moins de limitation, de ce que cette coopération peut signifier exactement.

Pouvoir de réquisition dans le cadre de la mise en œuvre de méthodes exceptionnelles

86. En ce qui concerne **ce pouvoir de réquisition**, le Comité ne parvient pas à déterminer quels types de collaboration relèvent du champ d'application. L'article 18/10, § 3/1 parle de « concours conformément à l'article 13/4 ». Cette dernière disposition ne donne cependant aucune précision à ce sujet. L'exposé des motifs indique qu'il s'agit d' *« d'experts ou d'acteurs externes disposant de compétences techniques, d'infrastructures ou de possibilités d'accès spécifiques qui sont essentiels à la bonne exécution de la mission »*.[76] Cette explication est largement insuffisante pour le Comité. D'autres exemples sont encore énumérés.[77] Cela semble toutefois insuffisant, d'autant plus que le projet de loi prévoit des sanctions pénales en cas de refus de collaborer. On peut notamment se demander si, par exemple, **toute personne peut être contrainte, en vertu du droit pénal, de mettre son domicile à la disposition de la VSSE ou du SGRS dans le cadre d'une mission d'observation (art. 18/11 L.R&S).** On peut également se demander si, par exemple, un serrurier s'expose à des poursuites pénales en vertu de cette disposition lorsqu'il refuse d'aider un service de renseignement à pénétrer dans un domicile ou un lieu privé (art. 18/12 L.R&S), ou si **un comptable ou un avocat s'expose à des poursuites s'il refuse de contribuer à la mise en place, par la VSSE ou le SGRS, d'une entreprise (frontstore), d'un système** visant à collecter des informations (art. 18/13 L.R&S). **Le Comité émet un avis défavorable et demande instamment que l'ensemble du dispositif soit entièrement revu en tenant compte des remarques formulées ou supprimé (REC-63).**

Se pose en outre la question de **la manière dont ce nouveau pouvoir de réquisition**, dans le cadre de l'utilisation de méthodes exceptionnelles, **s'articule avec les droits d'action déjà existants dans le cadre des méthodes exceptionnelles**. Il s'agit plus précisément du pouvoir de réquisitionner des opérateurs postaux (art. 18/14 L.R&S), des opérateurs de communications électroniques et fournisseurs d'un service de communications électroniques (art. 18/17 L.R&S), certaines institutions financières (art. 18/15 L.R&S), et certains experts en systèmes et services informatiques (art. 18/16 L.R&S).

[76] Exposé des motifs, p. 13.
[77] Exposé des motifs, p. 64.

87. Il est prévu à l'article 18/10, § 3/1 que ce concours peut être requis *« en cas de, soit danger grave pour l'intégrité physique d'une ou plusieurs personnes, soit d'activités en rapport avec le terrorisme ou avec les organisations criminelles »*. Le Comité rappelle tout d'abord que **les notions de « terrorisme » et d'« organisation criminelle »** ont, dans la Loi Renseignement, une définition qui leur est propre et qui est en partie plus large et, en partie, plus restrictive que celle qui leur est donnée dans le Code pénal. **Le Comité demande de préciser de quelle signification il s'agit (REC-64).** Il s'agit, en outre, de qualifications qui peuvent être mises à profit assez rapidement dans un certain contexte de renseignement.

Pouvoir de réquisition dans le cadre de missions d'entrave

88. En ce qui concerne **ce pouvoir de réquisition**, l'exposé des motifs indique *« que l'obligation de concours est plus large en cas d'entrave »*.[78] Toutefois, étant donné que la mission d'entrave – telle que décrite dans le projet d'article 7, 5° en art. 11, 7° – est très large et ne prévoit aucune mesure concrète, il en résulte que la portée de ce pouvoir de réquisition **n'est pratiquement pas limitée**. Cela pose particulièrement problème au regard du principe de légalité en matière pénale, surtout lorsque cette coopération s'accompagne de la commission d'infractions pénales.

89. La demande écrite du service de renseignement concerné adressée à la Commission BIM en vue d'obtenir son accord pour solliciter un concours dans le cadre d'une méthode exceptionnelle doit contenir plusieurs mentions obligatoires (*cf.* projet d'article 18/10, § 3/2, alinéa 2). Une de ces mentions est la suivante : *« soit de danger grave pour l'intégrité physique d'une ou plusieurs personnes, soit d'activités en rapport avec le terrorisme ou avec les organisations criminelles »* (point 3°). Le Comité constate que la demande écrite par le service de renseignement concerné à la Commission BIM afin d'obtenir son accord pour adresser une réquisition de concours dans le cadre d'une mission d'entrave ne comporte pas de justification de fond comparable (*cf.* projet d'article 19/6, § 2, alinéa 2). **Le Comité estime qu'il convient d'ajouter la même mention (REC-65).** Au regard de l'avis rendu sur la mission d'entrave, cela peut être décrit comme suit : « *la menace grave et actuelle qui pèse sur la sécurité nationale* ».

Les incriminations et les sanctions pénales y afférentes

90. Le projet de paragraphe 3/4 de l'article 18/10 L.R&S et le projet de paragraphe 5 de l'article 19/6 L.R&S contiennent **les incriminations et la sanction pénale y afférente pour les personnes qui refusent de prêter leur concours**.

Projet d'article 18/10, § 3/4:
« Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes (sic) 3/1 jusqu'au paragraphe 3/3 est punie d'une peine de niveau 1. ».

Projet d'article 19/6, § 5:
« Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er à 3 est punie d'une peine de niveau 1. ».
Par dérogation à l'alinéa 1, toute personne physique ou toute personne morale dont le concours peut être requis pour l'exécution des méthodes visées à l'article 18/2, § 1er et § 2 et qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er à 3 est punie d'une peine de niveau 2. Par dérogation à l'article 52 du Code pénal, l'amende à titre de peine accessoire s'élève à 200 euros au moins et à 160.000 euros au plus. ».

[78] Exposé des motifs, p. 79.

L'exposé des motifs ne fournit aucune précision à propos de ces deux dispositions. Le Comité considère qu'il existe néanmoins un besoin en la matière (REC-66). Concernant le projet d'article 18/10, § 3/4 le rapport entre l'incrimination et la sanction prévues ici et les incriminations et sanctions existantes définies à l'encontre des opérateurs postaux (art. 18/14, § 3 L.R&S), des opérateurs de réseaux de communication électroniques et de fournisseurs d'un service de communications électroniques (art. 18/17, § 3, alinéa 2 L.R&S), de certaines institutions financières (art. 18/15, § 4 L.R&S), et de certains experts en systèmes et services informatiques (art. 18/16, § 4 L.R&S), n'est pas clair, d'autant plus que le projet de loi prévoit un alourdissement de ces dernières sanctions (voir art. 48 du projet de loi). Cette dernière mesure se justifie à juste titre, selon le Comité, par une assimilation à l'infraction de « méconnaissance de l'obligation de collaborer à l'enquête (pénale) » (art. 655 CP-2024). **Le Comité recommande de préciser ce rapport dans l'exposé des motifs.**

En ce qui concerne le projet d'article 19/6, § 5, le champ d'application du deuxième alinéa est extrêmement flou. Il est stipulé que *« [p]ar dérogation à l'alinéa 1, »* – cet alinéa porte sur le refus de collaborer à une action d'entrave – *« toute personne physique ou toute personne morale dont le concours peut être requis pour l'exécution des méthodes visées à l'article 18/2, § 1er et 2 »* – Cette partie de la phrase porte sur la collaboration à apporter dans le cadre de méthodes de renseignement spécifiques et exceptionnelles – *« et qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er à 3 est punie (…) »*. **Le Comité recommande soit de supprimer cette disposition, soit de la reformuler et de la clarifier dans l'exposé des motifs (REC-67).**

Les tarifs

91. Le Comité se demande par ailleurs si l'article 18/18 L.R&S, qui porte sur **les tarifs** dont le service de renseignement en question doit s'acquitter pour la collaboration de tiers, s'applique également à la collaboration telle que visée au projet d'article 18/10, § 3/1 et suivants L.R&S. Cela semble être le cas, étant donné que les dispositions concernées font partie de la section 2. L'article 18/18 L.R&S dispose en effet que *« [l]e Roi fixe les tarifs rétribuant la collaboration des personnes physiques et des personnes morales les méthodes visées à l'article 16/2 et dans la sous-section 2, en tenant compte du coût réel de cette collaboration. »*. **Le Comité n'a trouvé aucune information à ce sujet dans l'exposé des motifs et demande des éclaircissements. Il est également demandé au gouvernement si l'arrêté royal existant s'applique ou s'il convient d'adopter un nouvel arrêté royal à cet effet (REC-68).**

Étant donné que le projet d'article 19/6 L.R&S ne relève pas de la sous-section 2, section 4, chapitre 3 de la Loi Renseignement, on peut en conclure que l'article 18/18 L.R&S ne s'applique pas en ce qui concerne le concours de tiers dans le cadre d'une entrave. Néanmoins, **le Comité recommande de prévoir également une réglementation distincte (REC-69).**

(12) CATÉGORIES PROFESSIONNELLES PROTÉGÉES

92. Le projet de loi **supprime la notification obligatoire de la Commission BIM aux présidents des Ordres des avocats[79], de l'Ordre des médecins et de l'Association des journalistes professionnels** préalablement à la mise en œuvre prévue d'une méthode spécifique ou exceptionnelle (suppression de l'article 18/2, § 3 et ajout d'un nouvel article 18/2/1, § 3). L'exposé des motifs justifie cette mesure comme suit : *"Cette notification n'a aucune composante substantielle : le président de l'association professionnelle n'a aucun pouvoir d'appréciation, ni le pouvoir d'intervenir contre l'utilisation de la méthode"*. Il est en outre prévu que *« (b)ien que la modification proposée rend les dispositions et procédure en vigueur plus efficaces et plus souples, elles ne remettent pas en cause les garanties offertes pour la protection des données d'un avocat, d'un médecin ou d'un journaliste*

[79] À savoir l'*Orde van de Vlaamse balies* et l'Ordre des barreaux francophones et germanophone.

couvertes par le secret professionnel ou le secret des sources ».[80] **Le Comité recommande de solliciter l'avis des ordres et de l'association mentionnés afin de vérifier si ce motif est valable (REC-70).**

93. Dans le cadre de la procédure particulière applicable à la collecte d'informations par des méthodes spécifiques et exceptionnelles, la question se pose toutefois de savoir **comment le président de la Commission BIM peut déterminer quelles informations déjà recueillies relèvent du secret professionnel et lesquelles n'en relèvent pas**. La procédure en question prévoit en effet que *« le président de la commission ou, en cas d'empêchement un autre membre de la Commission, vérifie si les données obtenues grâce à cette méthode, lorsqu'elles sont protégées par le secret professionnel de l'avocat ou du médecin ou par le secret des sources du journaliste, sont directement liées à la menace ».*

L'article 90*octies*, § 3 CIC, qui prévoit une procédure similaire dans le cadre de l'instruction pénale, résout cette question en imposant au juge d'instruction l'obligation de consulter, à cette fin, l'Ordre des avocats ou l'Ordre des médecins. **Il est recommandé d'adopter la même disposition, surtout si l'obligation de notification préalable est supprimée (REC-71).**

(13) SECRET (art. 36 L.R&S)

94. Le projet de loi étend le secret aux personnes « *à qui il est demandé d'apporter son concours* ». Le Comité se demande toutefois, au regard du § 2 de l'article 36 si le champ d'application – outre son élargissement en ce qui concerne les personnes mentionnées – est délibérément restreint en ce qui concerne les agents des services de renseignement.

L'actuel article 36, § 2 s'énonce comme :
« Le secret subsiste même lorsque les agents ont cessé leurs fonctions ou lorsque les personnes ne coopèrent plus avec les services. »

La proposition d'article 36, § 2 est formulée comme suit :
« Le secret subsiste même lorsque l'agent ou la personne visée à l'alinéa 1er cesse d'apporter son concours ou refuse d'apporter son concours. ».

Ainsi, **les mots « ont cessé leurs fonctions » sont supprimés** . Il s'agit là d'**une limitation du champ d'application de l'article 36, § 2.** De cette manière, les infractions pénales visées à l'article 43 L.R&S sont également limitées, compte tenu de la référence qui y est faite à « l'agent ou la personne visée à l'article 36 ».

Le Comité demande **soit de préciser dans l'exposé des motifs pourquoi le champ d'application concerné est restreint, soit de laisser tomber cette suppression (REC-72).**

(14) CONCERNANT L'ENQUÊTE DE SÉCURITÉ D'UN PARTENAIRE NON COHABITANT (projet d'article 16, § 4 L.C&HS)

95. Le Comité R/I constate qu'en exécution de sa décision DPA CPR/DPA/2026/01 du 3 février 2026 relative à un nouveau questionnaire de base de la VSSE, un cadre juridique clair est prévu pour les enquêtes de sécurité individuelles portant sur le ou les partenaires ne vivant pas sous le même toit qu'une personne devant obtenir une habilitation de sécurité et avec lesquels cette dernière entretient une relation durable. Le Comité est d'avis que cette disposition concilie au mieux les intérêts en matière de sécurité et la protection de la vie privée des

[80] Exposé des motifs, p. 11.

tiers. Le Comité fait toutefois remarquer que si le terme « relation durable » était (exclusivement) défini dans une directive du Conseil National de Sécurité en exécution de l'article 18, alinéa 5, Loi du 11 décembre 1998 relative à la classification (tel qu'annoncé dans l'exposé des motifs), celle-ci n'est pas opposable à la personne concernée, à son « partenaire », au Conseil d'État (par exemple en cas de décision de déclarer irrecevable la demande d'enquête de sécurité) ou à l'Organe de recours en matière habilitations et d'avis de sécurité (par exemple en cas de refus ou de retrait d'une habilitation de sécurité pour des faits liés à un partenaire). En effet, en vertu de cette disposition légale, de telles directives ne sont pas publiques. **Le Comité recommande de définir les termes « partenaire » et « relation durable » dans la loi, l'exposé des motifs ou dans une directive publique, de sorte que, dans un premier temps, chaque personne concernée puisse préalablement déterminer au mieux quelles sont les conséquences possibles d'une relation donnée pour une habilitation de sécurité (REC-73).** Cela revêt une importance particulière lorsqu'il existe une « composante étrangère » (résider ou avoir résidé à l'étranger ou posséder une autre nationalité), car cela peut avoir des conséquences directes sur une demande d'habilitation de sécurité.

(15) INTERVENTION LÉGISLATIVE REQUISE – PUBLICITÉ DE L'ADMINISTRATION

96. Le Comité rappelle à l'auteur l'arrêt de la Cour constitutionnelle par lequel l'obligation active de notification prévue à l'article 2, § 3 L.R&S (*infra*) a été annulée et que le législateur n'a pas encore rétablie. Une telle obligation, également connue sous le nom d'**« obligation de notification (active) »**, implique que sous certaines conditions, la VSSE et le SGRS doivent, de leur propre initiative, informer une personne visée qu'elle a fait l'objet d'une enquête, et plus précisément qu'une méthode de renseignement donnée lui a été appliquée dans le passé. En d'autres termes, une obligation de notification active signifie qu'un service de renseignement doit d'office divulguer en partie les résultats de son enquête et les informations dont il dispose concernant une personne (anciennement) visée.

La Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (en abrégé : Loi MRD) a instauré pour la première fois une obligation active de notification dans le chef de la VSSE et du SGRS. L'article 2, § 3 L.R&S dont il est question a cependant été annulé par la Cour constitutionnelle (nr. 145/2011). 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** (en abrégé : Loi MRD actualisée) a instauré pour la deuxième fois une telle obligation de notification. L'article 2, § 3 L.R&S a cependant été une nouvelle fois annulé en 2019 par la Cour constitutionnelle (n° 41/2019). **Le Comité recommande de rétablir la réglementation concernée en tenant compte de la jurisprudence de la Cour constitutionnelle (REC-74).**

97. Le Comité rappelle en outre à l'auteur l'article 7, § 3 de la Loi Classification qui stipule ce qui suit : *« Les organes de contrôle compétents de l'autorité d'origine sont déterminés par le Roi. »*. La Loi du 7 avril 2023[81] a instauré **une réglementation générale de déclassification** dans la Loi Classification. La loi prévoit des délais au cours desquels les autorités d'origine – c'est-à-dire les instances chargées de la classification – sont tenues de vérifier si la classification et le niveau de classification doivent encore être maintenus. L'article de loi en question stipule ce qui suit : *« En l'absence d'évaluation dans les dix ans, l'organe de contrôle compétent peut ordonner par écrit à l'autorité d'origine d'évaluer la classification dans les trois mois conformément aux alinéas 1er à 3 et 8 à 10. Si l'évaluation n'a pas lieu dans les trois mois après cet ordre écrit, la classification expire. »*. Dans son avis législatif du 22 juillet 2024 relatif au projet d'arrêté royal portant exécution de le Loi du 11 décembre 1998 relative à la Classification : *« Le Comité recommande, dans cet arrêté, d'exécuter l'article 7 § 3, qui prévoit que le Roi désigne les organes de contrôle compétents pour agir dans le cadre des évaluations établies*

[81] Loi du 7 avril 2023 modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.* 9 juin 2023).

par l'autorité d'origine en cas de déclassification ou de prolongation de la période de classification. ».[82] Le Comité constate que sa recommandation n'a pas été suivi d'effet. **Le Comité recommande de modifier la disposition législative concernée et de désigner directement dans la loi les organes de contrôle compétents (REC-75).**

(16) REMARQUES D'ORDRE LINGUISTIQUE CONCERNANT LA LOI RENSEIGNEMENT

98. La notion de « Directeur des Opérations VSSE » (REC-76). L'article 3, 18° L.R&S décrit le « Directeur des Opérations de la Sûreté de l'État » comme *« l'agent des services extérieurs de la Sûreté de l'État revêtu du grade de commissaire général qui est chargé de la direction des services extérieurs de la Sûreté de l'État »*. Au regard de l'arrêté royal du 18 août 2025 portant des dispositions diverses relatives aux membres du comité de direction de la Sûreté de l'État (*M.B.* 22 août 2025), cette disposition ne correspond plus à l'organisation réglementaire de la VSSE. Compte tenu des compétences attribuées par cet arrêté royal, il serait préférable de remplacer la notion de « Directeur des Opérations de la Sûreté de l'État » par la notion de « Directeur Opérationnel Renseignements de la Sûreté de l'État ». Dans ce cas, il serait préférable de remplacer cette description par *« l'agent de la Sûreté de l'État qui est chargé de la direction Renseignements Opérationnels de la Sûreté de l'État comme déterminé le Roi »*. Une telle description tient davantage compte de la fonction de mandat exercée par la personne concernée, ainsi que du type de membres du personnel placés sous son autorité et sa direction.

99. La dénomination de la Loi du 11 décembre 1998 (REC-77). Depuis la loi du 2 juin 2024 (*M.B.* 8 juillet 2024), la dénomination correcte est la « loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé ». **La Loi du 30 novembre 1998 contient plusieurs dispositions qui ne sont pas adaptées à la nouvelle dénomination** (à savoir les articles 13, § 4, 18/17, § 5, 21/1, § 3, 43/1, § 2, et 43/5, § 3).

(17) MÉTHODES DE RENSEIGNEMENT : CRÉATION D'UN CADRE JURIDIQUE POUR UN BAC À SABLE

100. Le projet de loi prévoit la mise en place d'un environnement d'un bac à sable (sandbox) pour les activités liées à l'intelligence artificielle (*supra*). **Il serait cohérent de prévoir également un cadre juridique pour bac à sable dédié aux méthodes MRD**, compte tenu de leur complexité technique et de leur impact potentiel sur les droits fondamentaux. Un tel mécanisme permettrait de tester, d'évaluer et de définir un cadre pour ces méthodes MRD avant leur déploiement opérationnel.

En outre, les services de renseignement acquièrent régulièrement du nouveau matériel. Des formations sont également dispensées sur les méthodes ordinaires, dans le cadre desquelles de véritables données à caractère personnel sont collectées (par exemple lors de la formation HUMINT). Il existe une insécurité juridique quant à la manière dont ces formations doivent être traitées. Les critères relatifs à la menace, à la proportionnalité ou à la subsidiarité ne peuvent pas être appliqués. **Le Comité propose de mettre en place une mesure d'appui prévoyant que la Commission BIM et le Comité soient préalablement informés des exercices et des tests, et que les données collectées soient immédiatement et systématiquement détruites après l'exercice ou le test (REC-78).**

[82] Avis n°008/CPR-ACC/2024 du 22 juillet 2024 relatif au projet d'arrêté royal pris en exécution de la Loi du 11 décembre 1998 relative à la classification, p. 9.

(18) MODALITÉS DU CONTRÔLE

101. Le Comité est une institution indépendante. Cette indépendance et le caractère effectif du contrôle sont des conditions qui ont été reconnues comme essentielles à la constitutionnalité des normes dont le Comité R/I assure le contrôle (*cf.* les arrêts n°145/2011, 41/2019, 27/2020 et 134/2025 de la Cour constitutionnelle). L'augmentation des moyens d'action et de collecte des services de renseignement doit naturellement s'accompagner d'un élargissement des compétences des autorités d'autorisation et de contrôle que sont la Commission BIM et le Comité. Au fil des ans, les compétences se sont multipliées[83] et les modalités d'exercice de celles-ci varient fortement, résultant ainsi en une multitudes de processus différents difficiles à mettre en œuvre avec les moyens techniques et humains du Comité. Cette augmentation des moyens des services, et son corollaire de l'ajout de diverses compétences au Comité, n'a pas été accompagnée d'une refonte structurelle des moyens de contrôle et de la capacité d'obtenir de manière simple et directe des informations qui sont pertinentes pour un ou plusieurs des contrôles (éventuellement de façon transversale). En d'autres termes, la multiplicité des compétences et des manières d'exercer celles-ci rendent compliqué le contrôlé exercé par le Comité. Pour cette raison, des mesures structurelles et transversales sont jugées nécessaires par le Comité pour maintenir un contrôle effectif sur les services de renseignement.

102. À ce titre, **le Comité recommande de modifier la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement afin d'y insérer différentes dispositions**. Ces modifications, présentées **en annexe** renforcent la légitimité démocratique des services de renseignement en permettant une auditabilité effective, rassurant ainsi les autorités politiques responsables et le public quant au respect des droits fondamentaux tout en préservant leur efficacité opérationnelle. (**REC-79**).

Bruxelles, 03/06/2026

POUR LE COMITÉ R/I

Vanessa SAMAIN
Présidente

Frédéric GIVRON
Greffier

[83] À savoir le contrôle par enquête ou traitement de plaintes de la légalité, de l'efficacité et de la coordination ; le rôle d'autorité de protection des données, le traitement des signalements d'atteinte à l'intégrité, le contrôle a posteriori des méthodes particulières de recueil des données, le contrôle de certaines mesures ordinaires et des méthodes de protection et d'appui, etc.